Tätigkeitsbericht 2011

des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein

Berichtszeitraum: 2010, Redaktionsschluss: 15.02.2011
Landtagsdrucksache 17/1220

(33. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz)

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Impressum

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel

Mail: mail@datenschutzzentrum.de
Web: www.datenschutzzentrum.de

Satz und Lektorat: Gunna Westphal, Kiel
Illustrationen: Reinhard Alff, Dortmund
Umschlaggestaltung: Martin Papp, Eyekey Design, Kiel
Druck: Schmidt & Klaunig, Kiel

Inhaltsverzeichnis

1 Datenschutz in Schleswig-Holstein



Nach den turbulenten Jahren 2008 und 2009, in denen sich Datenschutzskandale und öffentliche Kontroversen zum Schutz der Privatsphäre und der Persönlichkeitsrechte im „digitalen Raum" lückenlos und überlappend aneinanderreihten, war das Jahr 2010 ein vergleichsweise ruhiges Jahr für den Datenschutz. Dies hatte jedoch weniger seinen Grund darin, dass die Verstöße weniger geworden sind, sondern es trat ein gewisser Gewöhnungseffekt ein, der nach dem Bekanntwerden jedes neuen Datenlecks aber nicht zu Desinteresse wegen Abstumpfung führte. Vielmehr wurde das aufgeregte Hüpfen von einem Erstaunen zur nächsten Empörung zumindest teilweise abgelöst durch die **Suche nach Lösungen** der ins Auge springenden Probleme.

Dabei ist erfreulicherweise festzustellen, dass bei der Suche nach Lösungen nicht auf alte Reaktionsmuster zurückgegriffen wurde – den Ruf nach dem starken Staat oder das Hoffen auf die selbstheilenden Kräfte des ungeregelten Marktes. Vielmehr ist die Ambivalenz der modernen Informationstechnik fest im öffentlichen und politischen Bewusstsein verankert – einerseits als Tor zu neuen Freiheiten bei der Information, der Kommunikation, der Freizeitgestaltung, dem politischen Engagement und der beruflichen und wirtschaftlichen Betätigung, andererseits als Abgrund für neue Formen der Kriminalität, der Persönlichkeitsverletzungen, der Manipulation und Diskriminierung, der Unterdrückung und gar der Kriegsführung. Diese Ambivalenz erlaubt keine einfachen und schnellen Antworten, sondern verlangt nach qualifizierten Lösungen. Die Probleme der hoch technisierten Informationsgesellschaft lassen sich **nicht mit symbolischen Maßnahmen** lösen, sondern nur unter Mobilisierung der Technik selbst, einer freiheitlichen Kultur, organisatorischen Vorkehrungen und – auch neuen – rechtlichen Regelungen.

Hier sehen der Datenschutz allgemein und das Unabhängige Landeszentrum für Datenschutz (ULD) ihre Aufgabe und Legitimation: angesichts des rasanten technischen Fortschritts und der unübersichtlicher werdenden Informationswelt unter Wahrung der demokratischen und freiheitlichen Werte die Probleme zu analysieren und technische, organisatorische und rechtliche Lösungen zu suchen, zu finden und umzusetzen. Dabei dringt einem täglich ins Bewusstsein, dass bei allen technischen, organisatorischen und rechtlichen Rahmenbedingungen das Hauptproblem und die **Hauptlösung die Menschen selbst** sind. Diese Erkenntnis hat zur zwangsläufigen Konsequenz geführt, Medienkompetenz zu vermitteln. Medienkompetenz ist aber nicht nur das mechanische Beherrschen von Informationstechnik. Dazu gehört auch ein neues informationsgesellschaftliches Bewusst-

sein mit neuen sozialen Verantwortlichkeiten, neuen Pflichten und neuen Werten. Dabei handelt es sich um nichts völlig Neues, sondern um die alten Verantwortlichkeiten, Pflichten und Werte in einem neuen digitalen Gewand. Das ULD hat vor diesem Hintergrund die Sommerakademie 2010 mit dem Titel „Codex digitalis“ durchgeführt (32. TB, Tz. 2.1).

Dieser Bedeutungswandel ist in der Wirtschaft längst angekommen. Informationstechnik (IT) ist zum ökonomischen Motor geworden. Die Lebenswirklichkeit von immer mehr Menschen wird davon geprägt. Die Medien greifen die neuen Konflikte und Herausforderungen mit neuen Akteuren begierig auf und suchen auf die neuen Fragen Antworten. Symptomatisch hierfür war die das vergangene Jahr stark prägende Diskussion um die Veröffentlichung von Dokumenten durch WikiLeaks im Internet, die sich um die zentrale Frage drehte, welche legitimen Geheimnisse es in der globalen Informationsgesellschaft geben kann, muss und darf – im politischen, wirtschaftlichen und privaten Raum. Als weitere Frage drängte sich sogleich die nach der technischen Sicherung von Staatsgeheimnissen, von Betriebs- und Geschäftsgeheimnissen und der Privatsphäre auf. Zu diesen Fragen Antworten zu geben ist **Aufgabe der Datenschutz- und Informationsfreiheitsbeauftragten** – also auch des ULD.

Erstaunlich ist, dass die gefundenen Antworten sich nur noch begrenzt in das klassische politische Spektrum von links über die Mitte bis nach rechts einordnen lassen. Dies darf nicht zur Folge haben, dass nun statt der Ideologen die Technokraten das Schicksal unserer Gesellschaft bestimmen. Technik und deren Beherrschung müssen weiterhin instrumentellen Charakter bewahren und dürfen keine ungezügelte, sich selbst gestaltende Eigendynamik entwickeln. Hierüber zu wachen ist nicht nur Aufgabe der kritischen Öffentlichkeit und der Politik, nicht nur die der Datenschutz- und Informationsfreiheitsbeauftragten, sondern von allen Betroffenen und Beteiligten. Schleswig-Holstein hat sich in der Vergangenheit dieser politischen Herausforderungen in vorbildlicher Weise angenommen. Dies zeigte sich z. B. im engagierten Aufgreifen des Konfliktes um die Geodatendienste von Google, bei dem der Innen- und Rechtsausschuss des Landtages – lange bevor das Thema in der Bundespolitik angekommen war – intervenierte.


https://www.datenschutzzentrum.de/geodaten/google-landtag.html

Weiterhin wurde dies jüngst deutlich durch die Thematisierung der „**Netzneutralität**“ durch den Europaausschuss: Die Informationstechnik ist nicht nur eine Herausforderung für die Freiheitsrechte, sondern auch Auslöser neuer Verteilungskämpfe und damit eine Herausforderung zur Wahrung der Gleichheitsrechte und zur Verhinderung von Diskriminierungen. Auch insofern ist die Politik zur Problemanalyse und Gestaltung aufgerufen.


http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/1600/umdruck-17-1645.pdf

1.1 LDSG – Fortschritte sind nötig und möglich

Das Landesdatenschutzgesetz muss geändert werden, nachdem der Europäische Gerichtshof festgestellt hat, dass die deutschen Regelungen zur Datenschutzaufsicht mit europäischem Recht nicht vereinbar sind. Dies sollte Anlass sein, eine Generalüberholung des in die Jahre gekommenen Gesetzes vorzunehmen.

Als das neue Landesdatenschutzgesetz (LDSG) vor elf Jahren in Kraft trat, war es unbestritten eines der modernsten und fortschrittlichsten allgemeinen Datenschutzregelungen. Die **Technikentwicklung und die Datenverarbeitungspraxis** machen aber eine regelmäßige Revision nötig. Nachdem im März 2010 der Europäische Gerichtshof (EuGH) die Bundesrepublik Deutschland verurteilt hatte, weil ihre Datenschutzaufsicht in den Ländern europarechtswidrig ist, weil sie nicht unabhängig genug ist, war klar, dass das LDSG geändert werden muss.

Die Europäische Datenschutzrichtlinie sieht vor, dass die Kontrollstellen für den Datenschutz ihre Aufgaben „**in völliger Unabhängigkeit**“ wahrnehmen. Der EuGH stellte nun klar, dass die Kontrollstellen als „Hüter der Grundrechte und Grundfreiheiten objektiv und unparteiisch“ handeln müssen, was voraussetzt, dass sie „vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein“ müssen. Diese Unabhängigkeit schließt, so der EuGH, „jede Anordnung und jede äußere Einflussnahme, sei sie unmittelbar oder mittelbar“ aus.

Das **Unabhängige Landeszentrum für Datenschutz** (ULD) trägt die Unabhängigkeit schon im Namen. Auch in der Praxis wurden einige offensichtliche Einflussnahmeversuche von Unternehmen durch die Landesregierung jeweils klar zurückgewiesen. Doch sieht das LDSG im nicht öffentlichen Bereich die Rechtsaufsicht des Innenministeriums vor. Dies ist nach dem Urteil des EuGH nicht mehr möglich. Allenfalls die Dienstaufsicht des Ministerpräsidenten, soweit sie sich, ähnlich wie bei Richtern, auf Formelles und auf schwere Dienstvergehen beschränkt und nicht den Inhalt von Entscheidungen erfasst, ist nach dem Urteil des EuGH hinnehmbar.

Die nötigen Änderungen zur Anpassung des LDSG an die Rechtsprechung des EuGH sind gering. Über zehn Jahre Erfahrung mit dem LDSG haben im ULD eine Liste von Punkten entstehen lassen, bei denen Rechtsänderungen dringend notwendig oder zumindest wünschenswert sind. In Absprache mit dem Innenministerium erarbeiteten wir **Änderungsvorschläge für das LDSG**, die wir dem Ministerium im August 2010 zuleiteten. Diese resultieren teilweise aus den bundesweiten Diskussionen über die Eckpunkte zur Modernisierung der Datenschutzrechte (Tz. 2.1). U. a. haben wir folgende Punkte benannt:

- Durch Aufgabenauslagerung und Privatisierung im öffentlichen Bereich sowie die Anhebung des Datenschutzniveaus im nicht öffentlichen Bereich kann eine Einschränkung des Anwendungsbereichs des LDSG vorgenommen werden.

- Die bisherige Regelung zur Datensicherheit enthält nicht mehr Einzelmaßnahmen, sondern Schutzziele. Diese wurden inzwischen weiterentwickelt und sind entsprechend fortzuschreiben.
- Die zunehmende Automation und die damit verbundene Erhöhung der Relevanz elektronisch verarbeiteter Daten macht eine Präzisierung der Protokollpflichten nötig.
- Die Veröffentlichung von Verfahrensverzeichnissen sollte gemäß den heute bestehenden Möglichkeiten über das Internet erfolgen.
- Behördliche Datenschutzbeauftragte haben sich bewährt, weshalb deren Bestellung obligatorisch werden muss. Nach entsprechenden Rechtsänderungen auf Bundesebene kann die Kontrollbefugnis auf besondere Amts- und Berufsgeheimnisse erstreckt werden.
- Die Unklarheiten zur Einwilligungsfähigkeit von Jugendlichen wird dadurch beendet, dass ausdrücklich auf die Einsichtsfähigkeit abgestellt wird, die in der Regel schon mit 16 Jahren besteht.
- Gemäß einer EuGH-Entscheidung muss eine Daten übermittelnde Stelle Auskunft über die Empfänger geben, weshalb diese zu dokumentieren sind.
- Durch Einfügung einer Regelung zur Veröffentlichung personenbezogener Daten im Internet wird hierfür eine klare Rechtsgrundlage geschaffen.
- Die Regelung zur Videoüberwachung sollte an die des BDSG angeglichen werden.
- Die bestehende Vorschrift zum Fernmessen und Fernwirken hat keine praktische Bedeutung mehr und kann wegfallen, ebenso wie die Regelung zur Dokumentation über Sekten.
- Gemäß den Normen auf nationaler und europäischer Ebene wird eine Informationspflicht gegenüber Datenschutzaufsicht bzw. Betroffenen bei unrechtmäßiger Übermittlung vorgeschlagen, die sogenannte Breach Notification.
- Die völlige Unabhängigkeit des ULD wird gemäß dem Urteil des EuGH rechtlich sichergestellt.
- Die Regelung einer angeforderten Datenschutzprüfung ohne Abschluss mit einer Zertifizierung wird ausdrücklich vorgesehen.
- Die Möglichkeiten zur Erhebung von Entgelten sind zu erweitern.
- Das ULD erhält die umfassende Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten nach dem Datenschutzrecht.

Kurz vor Redaktionsschluss hat uns das **Innenministerium des Landes** seine Überlegungen zur LDSG-Novellierung mitgeteilt, die weitgehend mit unseren Vorschlägen übereinstimmen.

Was ist zu tun?
Das LDSG sollte noch in dieser abgekürzten Legislaturperiode modernisiert werden, sodass es seinen innovativen und zukunftsgerichteten Charakter bewahrt.

1.2 Die Dienststelle

Nicht nur das LDSG ist in die Jahre gekommen, auch die Dienststelle des ULD bedarf einer kritischen Bestandsaufnahme und einer Zukunftsausrichtung. Dieses Ziel wird mit der Erstellung eines ULD-Konzepts verfolgt.

Die Arbeit einer Datenschutzbehörde bewegt sich immer in einem Spannungsverhältnis von **Anspruch und Wirklichkeit**. Nicht nur, dass die gesetzlichen Ansprüche mit der Realität der Datenverarbeitung in Einklang zu bringen sind, was Gesetzesänderungen oder eine Änderung der Praxis nötig macht, auch die Erwartungen der gesellschaftlich relevanten Gruppen – Bevölkerung, Politik, Wirtschaft Medien, Informatik, andere Behörden – werden durch die Verwaltungspraxis oft nicht erfüllt. Eine zentrale Restriktion der eigenen Arbeit sind bei zunehmenden Aufgaben die begrenzten Finanzen, die das Land für den Datenschutz zur Verfügung stellen kann. Die Krise des Landeshaushaltes hat latent eine Krise des Datenschutzes zur Folge.

Angesichts dessen hat das ULD ein **Konzept für die eigene Tätigkeit** erstellt, das nach einer Bestandsaufnahme des Datenschutzes und seiner Rahmenbedingungen die strategischen Ziele und die zu deren Erreichung nötigen Maßnahmen benennt. Das Konzept dient sowohl der internen Orientierung als auch der Kommunikation des Selbstverständnisses und der Vorgehensweise des ULD nach außen.

Das Konzept wurde im Rahmen eines dienststelleninternen mehrstufigen Diskurses erstellt. Eine Überprüfung der einzelnen Bereiche des ULD erbrachte das erfreuliche Resultat, dass die Grundausrichtung der bisherigen Arbeit den Anforderungen und Bedürfnissen schon in weitem Maße entspricht. Dennoch sind weitere **Justierungen angezeigt**.

Dies gilt zunächst unzweifelhaft für die Notwendigkeit einer Modernisierung des Rechtsrahmens auf Landes-, auf Bundes- und auf internationaler Ebene (Tz. 1.1, Tz. 2.1 bis Tz. 2.3). Bei der Aufgabenwahrnehmung kann durch Standardisierungen eine noch höhere Effizienz erreicht werden. Die Möglichkeiten von Kooperationen und zur Arbeitsteilung sind noch nicht ausgeschöpft. Die inhaltliche Ausrichtung auf internationale Fragen und auf die Schnittmengen zum Verbraucherschutz muss vertieft werden. Die Verschränkung der IT-Planung im Land und eines weiter zu etablierenden Datenschutzmanagements kann nicht nur zur Erhöhung des Datenschutzniveaus, sondern auch der Kosteneffizienz genutzt werden. Die Potenziale der Informationstechnik (IT) im ULD selbst lassen sich besser nutzen. Die Eigenfinanzierung des ULD sollte angesichts der prekären Haushaltslage weiterentwickelt und auch zu einer verbesserten Absicherung der dadurch geschaffenen zusätzlichen Arbeitsplätze genutzt werden. Dabei spielt die Datenschutzzertifizierung eine wichtige Rolle.

Bei der Umsetzung des Konzeptes bedarf das ULD der **externen Unterstützung** – der kontrollierten Behörden und Unternehmen, der Politik sowie der kooperierenden Stellen im Bereich Datenschutz, Verbraucherschutz und Medienkompetenz. Wir hoffen, mit der Veröffentlichung des ULD-Konzeptes eine Grundlage für den Austausch geschaffen und zugleich relevante Diskussionspunkte für die

weitere gemeinsame Arbeit im Interesse des Datenschutzes und der Informationsfreiheit benannt zu haben.



https://www.datenschutzzentrum.de/ldsh/konzept/

Was ist zu tun?
Das ULD wird das Konzept als Grundlage für die weitere Arbeit verwenden. Nach einem Zeitablauf von einigen Jahren ist zu prüfen, welche Änderungen und Weiterentwicklungen möglich und nötig sind.

2 Datenschutz − bundesweit



Die Musik beim Datenschutz spielte im Jahr 2010 vor allem im nationalen Bereich. Waren die Jahre 2008 und 2009 noch geprägt von der öffentlichen Überraschung über die Möglichkeiten und Risiken der Informationstechnik und von der Empörung über deren gesellschaftsschädliche Nutzung, etwa durch telekommunikativ aktive Abzocker, durch Vorstände von Großkonzernen oder durch dubiose Sicherheitsfirmen, so ist dies der Suche nach den dahinterstehenden Problemen und Lösungen gewichen. Diese **Problem- und Lösungsorientierung** äußerte sich in der Koalitionsvereinbarung auf Bundesebene, in der Einrichtung einer Enquetekommission des Bundestages (32. TB, Tz. 2.2), in einem Gesetzentwurf zum Beschäftigtendatenschutz (Tz. 5.1), in Vorbereitungen für eine Stiftung Datenschutz (Tz. 2.3), in „14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft“ des Bundesinnenministers, in Gesetzesinitiativen zu Veröffentlichungen im Internet oder in ersten Versuchen der Selbstregulierung der Internetwirtschaft (Tz. 2.2).

Nun lässt sich nicht behaupten, dass sämtliche Versuche, Anworten auf die neuen Herausforderungen zu geben, ins Schwarze getroffen hätten. Ein Beispiel hierfür sind die **14 Thesen des Bundesinnenministers**: Diese basieren darauf, dass die Selbstregulierung Vorrang vor staatlicher Normierung haben soll. So berechtigt die Kritik an den bisherigen detaillistischen Regulierungsversuchen der Informationstechnik ist, so unbegründet ist die Hoffnung, dass eine profitorientierte Wirtschaft von sich aus gemeinsame Werte verfolgen würde, die in den Thesen zutreffend benannt werden: „Freiheit, Selbstbestimmung und Eigenverantwortung, Gebot des gegenseitigen Respekts und der Rücksichtnahme sowie der Chancengleichheit und Solidarität“. Es ist unrealistisch, von der Wirtschaft zu erwarten – so der Minister anlässlich des Spitzengesprächs „Digitalisierung von Stadt und Land“ im September 2010 –, „nicht danach zu streben, den gesetzlichen Rahmen stets zugunsten ihres Geschäftes auszuschöpfen“. Zwar ist es richtig, dass vor der Schaffung neuer Gesetze die Anwendung der bestehenden zur Lösung neuer Probleme versucht werden sollte. Gerade im Bereich des Datenschutzes hat sich aber gezeigt, dass unser aus den 90er-Jahren stammendes Recht keine adäquaten Antworten auf die brennenden Probleme geben kann. Nur ein verbindlicher gesetzlicher Rahmen kann eine valide Grundlage für Selbstregulierung sein.

2.1 „Ein modernes Datenschutzrecht für das 21. Jahrhundert“

Auf Initiative des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) formte sich Mitte 2009 eine Arbeitsgruppe zur Erarbeitung von

Vorschlägen für eine umfassende Modernisierung des Datenschutzrechts. Im März 2010 wurde als Ergebnis das **Eckpunktepapier** „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ vorgelegt. Um das Datenschutzrecht an die technische Entwicklung anzupassen, schlagen die Datenschutzbeauftragten des Bundes und der Länder eine Reihe von rechtlichen Änderungen vor. Gefordert werden z. B. eine verstärkte rechtliche Kontrolle von Profilbildungen oder eine effektive Regelung der Datenverarbeitung bei Cloud Computing. Die technisch-organisatorischen Maßnahmen sollen an dem Konzept von Schutzzielen ausgerichtet werden. Die Betroffenenrechte sind zu stärken. Die Einwilligung soll ihrem eigentlichen Sinn entsprechend eine freiwillige Willenserklärung sein. Insbesondere im Hinblick auf das Internet und die dadurch drohenden Gefährdungen schlägt das Papier spezifische bestimmte Maßnahmen vor. Dazu gehört „Privacy by Default“, d. h., Internetdienste müssen in der Grundeinstellung standardmäßig ein Optimum an Datenschutz bieten, von dem nur durch Einzelentscheidung des Nutzers abgewichen werden kann.

Das ULD leistete zu dem Eckpunktepapier Beiträge zur Verbesserung und **Effektivierung der Datenschutzkontrolle**, z. B. durch Änderungen im Bundesdatenschutzgesetz (BDSG), welche die Aufsichtsbehörden in die Lage versetzen, eine wirksame Kontrolle der Datenverarbeitung durchzuführen und gegebenenfalls angemessene Sanktionen zu verhängen. Auch nach den kürzlichen Änderungen im BDSG gibt es weiterhin erheblichen Nachholbedarf. Es ist zu hoffen, dass das Papier die Datenschutzgesetzgebung der kommenden Jahre auf Bundes- und Landesebene beeinflussen und prägen wird.



http://www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/modernisierung.pdf

2.2 Eine rote Linie und ein Kodex

Die Suche nach einem Datenschutzrecht für das Internet erreichte kurz vor dem IT-Gipfel der Bundesregierung Ende 2010 ihren Höhepunkt in einem Gesetzesvorschlag des Bundesinnenministers und einem Selbstregulierungsvorschlag des Branchenverbandes BITKOM. Beides ist gut gemeint, die Gesetzesinitiative erweist sich jedoch als wenig tauglicher Versuch.

Die Auseinandersetzung um die Veröffentlichung von Straßenbildern durch Google im Internet führte zu einem **Gesetzentwurf des Bundesrates** mit einer Spezialregelung im Bundesdatenschutzgesetz (BDSG) zur „geschäftsmäßigen Datenerhebung und -speicherung im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Geodaten zum Zweck der Bereithaltung fotografischer oder filmischer Panoramaaufnahmen im Internet zum Abruf für jedermann oder zur Übermittlung an jedermann“. So sperrig der Titel dieses Entwurfes daherkommt, so sperrig ist auch dessen Regelungsinhalt: Der Gesetzesvorschlag füllt eine ganze eng beschriebene DIN-A4-Seite. So unpraktikabel der konkrete Vorschlag ist, so richtig ist ein darin enthaltener Gedanke: die Aufnahme eines rechtlich verpflichtenden Widerspruchsrechts gegen Bilddarstellungen. Zu kurz gegriffen ist die Beschränkung der Regelung auf georeferenzierte Panoramadienste im Internet.

Dies konnte und durfte nicht das letzte Wort des Gesetzgebers sein. Mit dieser Erkenntnis lud die Bundesregierung im September 2010 zu einem „**Datenschutzgipfel**“ ein und forderte dort von der Internetwirtschaft, sich durch Selbstregulierung in Form eines Datenschutzkodexes selbst Grenzen zu setzen. Weiterhin wurde ein eine rote Linie ziehender Gesetzentwurf angekündigt.

In dieser Situation sah sich das ULD veranlasst, **einen eigenen Gesetzentwurf** in die Diskussion einzubringen, mit dem nicht nur die Veröffentlichung von Geodaten, sondern von Personendaten jeder Form im Netz einer rechtssicheren und zugleich entwicklungsoffenen Regulierung zugeführt werden soll. Im Zentrum des Vorschlags steht die Einführung eines neuen Paragrafen im BDSG, der die elektronische Veröffentlichung von personenbezogenen Daten von einer Abwägung zwischen dem Grundrecht auf Meinungsfreiheit und dem Datenschutz abhängig macht. Zwecks beschleunigter Konfliktregelung sind digitale Beschwerde- und Prüfungsrechte vorgesehen. Folgende weitere Punkte sind geplant:

- Verantwortlichkeit von inländischen Konzernunternehmen bei einem Sitz der Internetfirma außerhalb Europas,
- Abgrenzung von reinen Sachdaten zu personenbezogenen Daten,
- Anpassung der Definition der „verantwortlichen Stelle“ an die Regelungen des Telemediengesetzes (TMG),
- Einführung des Prinzips „Privacy by Default“, also der Pflicht zu datenschutzfreundlichen Grundeinstellungen für Anbieter von Telemediendiensten,
- Regelung der elektronischen Einwilligung.

Die neue **Regelung zur Veröffentlichung** verlangt von jedem Menschen wie jeder Stelle bei Bereitstellung personenbezogener Daten zum Abruf im Internet eine Abwägung zwischen Veröffentlichungsinteresse und den schutzwürdigen Interessen des oder der Betroffenen. Ein Überwiegen letzterer wird bei besonderen Arten personenbezogener Daten, also z. B. Gesundheitsdaten, unterstellt. Da an einer Abwägung kein Weg vorbeigeht, hierfür aber keine spezifischen Abwägungskriterien festgelegt werden können, da die Fallkonstellationen so vielfältig wie das Internet sind, wählt der Entwurf einen prozeduralen Weg der Konfliktlösung: Widerspricht der Betroffene, so muss der Impressumspflichtige nach dem Telemediengesetz (TMG) umgehend reagieren. Tut er dies nicht, so wendet sich die Rechtmäßigkeitsvermutung gegen die Veröffentlichung. Ist ein Widerspruch aus einer allgemein zugänglichen Quelle erkennbar, so muss dieser beachtet werden. Um zumindest bei Massenverarbeitungen à la Google Street View den Betroffenen vorab ein Chance auf Widerspruch zu geben, wird eine Benachrichtigung auf einer Internetseite Pflicht. Zudem soll durch Verknüpfung des personenbezogenen Datums bei der ursprünglichen Veröffentlichung im Internet mit einem Meta-Löschdatum die Chance zur Realisierung der „Gnade des Vergessens“ erhöht werden. An einer behördlichen Konfliktlösung durch die Datenschutzaufsicht, die natürlich in einem hohen Maße Opportunität walten lassen muss, geht kein Weg vorbei. Die Diskussion über die Vorschläge hat schon zu ersten Modifikationen des ersten Entwurfs geführt. Gefordert sind jetzt die Politik und die Datenschutz-Community.



https://www.datenschutzzentrum.de/presse/20101027-gesetzesvorschlag-internet-regulierung.htm

Anfang Dezember 2010 stellten dann der Bundesminister des Innern (BMI) und der Branchenverband BITKOM ihre Vorschläge der Öffentlichkeit vor. Vom BMI ist auch ein zusätzlicher Paragraf im BDSG über „unzulässige Veröffentlichungen in Telemedien“ vorgesehen, der ebenso wie der ULD-Vorschlag eine umfassende Regelung anstrebt. Materiell ist der **BMI-Vorschlag** jedoch enttäuschend: Indem er nur eine absolut nicht zu überschreitende rote Linie markiert, regelt er Selbstverständlichkeiten, die schon heute gelten: das Verbot besonders schwerer Eingriffe in das Persönlichkeitsrecht, insbesondere durch das geschäftsmäßige Zusammentragen von Daten zur Bildung von Persönlichkeits- oder Bewegungsprofilen oder in Form von Ehrverletzungen. Der Vorschlag provoziert mehr Fragen, als er Antworten gibt, wenn eine Datenverarbeitung die rote Linie nicht überschreitet, aber dennoch unverhältnismäßig das Persönlichkeitsrecht von Betroffenen verletzt: Soll das zulässig sein? Wenn nein, mit welcher Begründung bzw. Rechtfertigung, wenn ja, nach welcher Regelung?

Der **Vorschlag des BITKOM** hat eine höhere praktische Relevanz. In einem Kodex als Instrument der Selbstverpflichtung gibt sich die Branche bei georeferenzierten Panoramadiensten im Internet bestimmte Regelungen. Im Mittelpunkt steht eine zentrale Informations- und Widerspruchsstelle, über die Bürgerinnen und Bürger ihre informationelle Selbstbestimmung wahrnehmen sollen. Zudem ist die Verpixelung von Gesichern und Kfz-Kennzeichen vorgesehen. Richtig weiterführend ist aber auch dieser Vorschlag nicht. Die Auflagen des Düsseldorfer Kreises als Zusammenschluss der Aufsichtsbehörden zum Dienst Google Street View gehen in ihren 13 Punkten in mancher Hinsicht weiter. Es besteht bei Google vorab ein Widerspruchsrecht; beanstandete Rohdaten müssen gelöscht werden. Es erfolgte keine sanktionslose unverbindliche Festlegung; vielmehr leiten sich die 13 Punkte nach dem Verständnis der Aufsichtsbehörden zwingend aus der bisher geltenden Abwägungsregelung ab, sodass sämtliche Sanktionsmittel des BDSG genutzt werden können. Positiv zu bewerten ist beim BITKOM-Kodex grundsätzlich der Ansatz der Selbstregulierung als flexibles Instrument für einen praktikablen Persönlichkeitsschutz. Doch kommt allzu viel Wasser in diesen Wein, weil ein Unternehmen sich von der freiwilligen Selbstverpflichtung einseitig entbinden kann, keine Bezugnahme zum gesetzlichen Rahmen erfolgt und nicht einmal die im BDSG vorgesehene Genehmigung als Verhaltensregel angedacht wurde. Insofern muss und kann nachgebessert werden. So könnte der Kodex zum Vorbild für Verhaltensregeln in anderen Bereichen der Internetdatenverarbeitung werden, z. B. bei Suchmaschinen, sozialen Netzwerken, Bewertungsportalen oder für Online-Archive.

Was ist zu tun?
Der Bundesgesetzgeber sollte kurzfristig eine umfassende Regelung zur Veröffentlichung personenbezogener Daten im Internet in Angriff nehmen und kann hierbei auf den ULD-Vorschlag zurückgreifen. Dies konkretisierend sollten zu spezifischen Fallgestaltungen verbindliche Verhaltensregeln der Branchenverbände erarbeitet werden.

2.3 Stiftung Datenschutz

Eine Stiftung Datenschutz soll künftig Audit- und Gütesiegelverfahren durchführen, vergleichende Tests vornehmen, Bildungsangebote bereitstellen und forschend den Datenschutz weiterentwickeln.

Im **schwarz-gelben Koalitionsvertrag** verabreden die Regierungsparteien für die laufende Legislaturperiode die Errichtung einer Stiftung Datenschutz mit dem Auftrag, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich Datenschutz zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern, ein Datenschutz-Audit zu entwickeln und datenschutzfreundliche Technik zu fördern, die „aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann".

Wir im ULD waren elektrisiert: Hier vereinbarten die Regierungsparteien genau das, was das ULD seit vielen Jahren propagiert und erfolgreich praktiziert – begrenzt durch die Möglichkeiten einer Landesbehörde. Daher haben wir uns umgehend an die **zuständigen Kabinettsmitglieder** im Bund gewandt, die Justizministerin und den Innenminister, erste Vorstellungen zur Stiftung formuliert und unsere Unterstützung angeboten. Die Rückmeldung der Justizministerin war grundsätzlich positiv. Sie stimmte damit überein, dass die Stiftung unabhängig sein müsse, signalisierte aber ebenso wie der Innenminister, dass die Überlegungen noch in einem frühen Stadium stecken (32. TB, Tz. 9.1).

Die Grundidee der Stiftung Datenschutz ist bestechend: Statt wie bei Datenschutzkontrollen Datenschutzverstößen repressiv hinterherzulaufen, soll **Datenschutz präventiv implementiert** und zu einem Wettbewerbsfaktor gemacht werden. Hierfür bedarf es Transparenz, Kompetenz und Unabhängigkeit. Dass dies rechtlich nicht gewährleistet wurde, war der Grund für das Scheitern des ersten Entwurfes eines Auditgesetzes der alten Bundesregierung (31. TB, Tz. 9.1).

Der **Bedarf** insbesondere an einer unabhängigen qualifizierten Zertifizierung erweist sich derzeit an allen Ecken und Enden personenbezogener Datenverarbeitung – bei den De-Mail-Diensten (Tz. 9.2.3) ebenso wie bei sensiblen Internetangeboten wie Bewertungsportalen (Tz. 4.6.9), sozialen Netzwerken oder Auswertern für Zwecke der zielgerichteten Internetwerbung, bei komplexen Forschungsdatenbanken ebenso wie bei Angeboten des E-Government. Die technischen und rechtlichen Datenschutzanforderungen an vertrauenswürdige Informationstechnik sind derart hoch und komplex, dass weder die Bürgerinnen und Bürger als Nutzende oder Betroffene noch viele Anwender die notwendigen Kompetenzen und Kapazitäten für eine fundierte Bewertung haben. Hier kann eine bundesweit agierende Stelle segensreich wirken, vorausgesetzt sie genießt das Vertrauen der Beteiligten wie der Öffentlichkeit.

Die weitere öffentliche Diskussion zeigte, dass die Stiftungsidee alles andere als unumstritten ist. Stellen, die Markttests, Bildungsmaßnahmen oder Zertifizierungen durchführen, können darin eine potenzielle Konkurrenz sehen. Vor allem sind es die vielen **offenen Fragen**, die Skeptikern Nahrung geben: Soll es sich um eine öffentliche oder private Stiftung handeln? Wie hoch soll das Stiftungskapital und

der verfügbare finanzielle Rahmen sein? Kann bei einer Wirtschaftsfinanzierung eine hinreichende Unabhängigkeit gewährleistet werden? Für die Datenschutzkontrollstellen besonders wichtig ist die Frage, wie das Verhältnis zwischen Kontrolle und Auditierung bzw. Zertifizierung ausgestaltet wird.

Inzwischen liegen die **ersten Antworten** vor. Die Stiftung soll offensichtlich privatrechtlich – unabhängig und staatsfern – organisiert sein. Der Haushaltsausschuss des Deutschen Bundestages hat für die Errichtung zehn Millionen Euro Kapital bereitgestellt. Im Jahr 2011 soll die Stiftung nach dem Willen der Koalitionsfraktionen den Betrieb aufnehmen, wobei aber zunächst das besonders heikle, aber zugleich besonders wichtige Zertifizierungsgeschäft zurückgestellt werden soll.

Auditierungen und Zertifizierungen sind nach Ansicht des ULD auf nationaler Ebene von großer Wichtigkeit. Dabei muss eine enge Kooperation mit den Datenschutzkontrollstellen erfolgen, ohne dass aber deren Unabhängigkeit beeinträchtigt wird. Dies kann in der Form geschehen, dass die Stiftung einen beratenden Status bei den relevanten Aufsichtsgremien, insbesondere dem bundesweiten Zusammenschluss des Düsseldorfer Kreises, erhält. Bei der Zertifizierung ist eine unverbindliche Anhörung der Kontrollstellen kurz vor Abschluss sinnvoll, jedenfalls dann, wenn ein lokaler Bezug besteht. So kann in einem frühen Stadium vermieden werden, dass Zertifizierung und Datenschutzkontrolle zu stark voneinander abweichenden Ergebnissen kommen. Ein wichtiger Aspekt ist die gemeinsame Entwicklung von **Schutzprofilen bzw. Standards** für spezifische Anwendungen. Hier ist denkbar, dass gemeinsame Arbeitskreise der Kontrollstellen und der Stiftung Vorschläge entwickeln, die gemeinsam veröffentlicht werden. Die Ängste vor Konkurrenz zu anderen Einrichtungen, z. B. des Verbraucherschutzes, müssen ernst genommen und durch enge Kooperationen abgebaut werden.

Hinsichtlich der **Zertifizierung** durch die Stiftung kann weitgehend auf die zehnjährigen Erfahrungen des ULD zurückgegriffen werden. Das Konzept der Begutachtung durch akkreditierte private technische und rechtliche Sachverständige hat sich sowohl beim Gütesiegel des ULD (Tz. 9.2) wie auch beim Europäischen Datenschutz-Gütesiegel (EuroPriSe, Tz. 9.3) als wirkungsvoll erwiesen. Dringend nötig ist eine Qualitätsprüfung und abschließende Zertifizierung durch eine unabhängige Stelle und eine Veröffentlichung der wesentlichen Ergebnisse des Verfahrens. Die Zertifizierung durch eine Stiftung Datenschutz muss sich zugleich in den europäischen Rahmen einfügen. Das Europäische Gütesiegel befindet sich in einigen EU-Mitgliedstaaten derzeit im Planungsstadium. Es ist insofern von Vorteil, dass über das ULD als erster EuroPriSe-Zertifizierungsstelle deutscher Sachverstand beim Aufbau der Stiftung Datenschutz genutzt werden kann.

Die Erfahrungen des ULD mit seinen Aktivitäten in den Bereichen Zertifizierung, Bildung, Beratung und Forschung sind, dass diese sich finanziell selbst tragen können. Voraussetzung ist eine gute technische Infrastruktur und qualifiziertes Personal. In jedem Fall ist bei einer **Finanzierung** über private Geldgeber jede inhaltliche Einflussnahme zu verhindern. Schon der Ruch der finanziellen Abhängigkeit schädigt das Vertrauen der Öffentlichkeit an der Unparteilichkeit der Stiftung.

Was ist zu tun?
Die Etablierung der Stiftung Datenschutz sollte zügig vorangebracht werden. Dabei ist äußerster Wert auf Transparenz Qualität, Unabhängigkeit und Kooperation mit nahestehenden Einrichtungen zu legen.

2.4 Vorratsdatenspeicherung „light“?

Mit einem Urteil vom März 2010 hat das Bundesverfassungsgericht das Gesetz für verfassungswidrig erklärt, wonach Telekommunikationsanbieter zu einer sechsmonatigen Vorratsspeicherung von Verkehrsdaten verpflichtet wurden. Seitdem stehen sich Gegner und Befürworter kompromisslos gegenüber.

Das Bundesverfassungsgericht hat eine Vorratsspeicherung von Verkehrsdaten aus der Telekommunikation (TK) nicht grundsätzlich verworfen, wohl aber deren äußerste verfassungsrechtlichen Grenzen aufgezeigt. Auf **EU-Ebene** soll im Jahr 2011 eine Evaluation der Speicherpflicht erfolgen, wobei eine Änderung der europäischen Vorgaben nicht ausgeschlossen ist. Zudem soll der Europäische Gerichtshof überprüfen, ob die Vorratsdatenspeicherpflicht mit der EU-Grundrechtecharta in Einklang steht.

Es gehört zu den politischen Gestaltungspflichten, nicht das maximal Mögliche an Grundrechtseinschränkungen vorzusehen, sondern **das Nötige und Sinnvolle**. Angesichts des Umstandes, dass das Internet zum umfassenden Kommunikationsnetz der Zukunft wird, sind rechtliche, organisatorische und technische Rahmenbedingungen zu schaffen, die einerseits eine wirksame Gefahrenabwehr und Strafverfolgung ermöglichen, andererseits aber hierbei einen effektiven Grundrechtsschutz – insbesondere der unbescholtenen und nicht verdächtigen Masse der Bevölkerung – zu sichern.

Die Diskussion zur Vorratsdatenspeicherung entwickelt derweil geradezu irrationale Züge: Vertreter von Sicherheitsbehörden und diese unterstützende Politiker erwecken – ähnlich wie bei der Diskussion um die sogenannte Online-Durchsuchung – den falschen Eindruck, ohne eine maximale Regelung sei Strafverfolgung im Internet nicht mehr möglich. Vorgetragene Zahlen und Argumente sind oft nicht nachvollzieh- und überprüfbar. Zu wenig berücksichtigt wird, dass Strafverfolgung im Internet nicht von einem einzigen Instrument abhängt, sondern von einem effektiv eingesetzten **Mix von Maßnahmen**, wobei viele dieser Maßnahmen grundrechtsneutral sein können.

Vorschläge zum **schnellen „Einfrieren“ von Verkehrsdaten**, das sogenannte Quick Freeze, wird als unwirksam von vornherein verworfen. Nicht hinreichend berücksichtigt werden die zu geringe personelle Ausstattung mit qualifizierten Strafverfolgern, die im Internet- bzw. IT-Bereich tätig sind, die bisher nicht optimierten Meldewege von den Anzeigenden zur Polizei sowie zu privaten Internetdienstleistern und wieder zurück zur Polizei, zu aufwendige und zeitträchtige Verfahrensabläufe – auch bei für den Grundrechtsschutz unerlässlichen verfahrensrechtlichen Sicherungen wie z. B. bei richterlichen Prüfungen –, fehlende

Standards für die Durchführung und Priorisierung von Strafverfolgungsmaßnahmen und Mängel in der Internetstruktur bezüglich Datenschutz und Datensicherheit.

Den Verfechtern der Vorratsdatenspeicherung stehen sich politisch deren Gegner ebenso wenig kompromissbereit gegenüber. Sie ignorieren, dass insbesondere hinsichtlich Straftaten im Internet die **IP-Adresse** oft der einzige Ermittlungsansatz ist, um einen Täter zu identifizieren. Die IP-Adresse ist aber beileibe nicht das sensibelste Datum, das von der Speicherpflicht erfasst wird. Die Notwendigkeit anderer Verkehrsdaten, z. B. der Standortangaben, ist wenig begründet. Sowohl der geforderte Umfang der auf Vorrat zu speichernden Daten als auch die Mindestspeicherdauer von sechs Monaten wurden bisher nicht auf ihre Erforderlichkeit und Verhältnismäßigkeit hin überprüft.

Die Speicherpflicht von TK-Daten ist nicht die erste Maßnahme einer anlasslosen Vorratsdatenverarbeitung für Zwecke der Strafverfolgung, ohne dass eine **wissenschaftliche Evaluation** vorgenommen wurde. Ebenso verhält es sich bei der präventiven Erfassung von Mobilfunkanschlüssen und der Bereitstellung und Auswertung von Fluggast- oder Finanztransaktionsdaten durch US-Sicherheitsbehörden (30. TB, Tz. 11.1; 32. TB, Tz. 11.3). Ohne Evaluation unter Berücksichtigung aller relevanten Parameter ist eine Optimierung zwischen den Zielen der Strafverfolgung und des Grundrechtsschutzes nicht möglich. In einer offenen Gesellschaft führt das Streben nach hundertprozentiger Sicherheit zum Tod aller Freiheit und nicht zum Erfolg.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und das ULD regten an, die Pflicht zur Speicherung auf **bestimmte Verkehrsdaten und auf eine kurze Dauer** zu beschränken. Zwar wurde dieses Eintreten für eine Vorratsdatenspeicherung „light“ von anderen Datenschützern heftig kritisiert. Doch ist auch von dieser Seite anzuerkennen, dass der Polizei wirksame Strafverfolgung im Internet möglich sein muss. Mit einem offenen Brief forderte das ULD den Präsidenten des BKA und Polizeiverbände auf, hierüber im Detail zu diskutieren und so die aktuelle politische Blockade bei diesem Thema aufzulösen. Diese Blockade kann in niemandes Interesse liegen. Die Gesprächsangebote des ULD fielen auf fruchtbaren Boden. In einem Vorschlag des Bundesjustizministeriums zur Vorratsdatenspeicherung sind unsere Anregungen berücksichtigt.



https://www.datenschutzzentrum.de/presse/20101123-offener-brief-vorratsdatenspeicherung.htm

Was ist zu tun?
Alle Beteiligten müssen sich gemeinsam an einen Tisch setzen, um effektive grundrechtsverträgliche Vorgehensweisen zur Bekämpfung der Kriminalität im Internet zu entwickeln.

3 Reauditierung Schleswig-Holsteinischer Landtag

Ziel eines Konzeptes für das Zutrittssystem und die Videoüberwachung des Landtages muss es sein, im aus Sicherheitsgründen äußerst sensiblen Parlament ein Höchstmaß an Gefahrenvorsorge zu realisieren, ohne dass hierbei Bürgernähe und Grundrechtskonformität leiden.

Die erstmalige Zertifizierung des Zutrittsberechtigungssystems erfolgte durch das ULD im Jahr 2004 (27. TB, Tz. 3.1), die der Videoüberwachung im Jahr 2006 (29. TB, Tz. 3.1). Die Dienst- und Verfahrensanweisungen wurden seitdem überarbeitet und der leicht geänderten Hardwareausstattung angepasst. Beim mit Funktechnologie arbeitenden Zutrittsberechtigungssystem wird weiterhin verhindert, dass durch die Nutzungsdaten der Zutrittsausweise Bewegungs- und Kontaktprofile, z. B. von Abgeordneten oder Journalisten, erstellt werden können. **Datenschutzfreundliche Merkmale** der eingesetzten Videoüberwachung sind die Ausblendung der für die Parlamentssicherheit nicht relevanten Verkehrsbereiche, ein differenziertes Zugangs- und Nutzungskonzept zu den Daten und Bildern, eine Löschroutine und öffentliche Hinweise auf den Technikeinsatz.

Das Zutrittsberechtigungssystem und die Videoüberwachung des Landtages sind aus Datenschutzsicht **vorbildlich**. Ein besonderes Qualitätsmerkmal ist das Datenschutzmanagement mit einem Datenschutzgremium, über das eine eigenständige unabhängige Kontrolle erfolgt. Bei der Rezertifizierung hat sich gezeigt, dass dieses Datenschutzmanagement nachhaltig funktioniert. Der Schleswig-Holsteinische Landtag ist bundesweit das einzige Parlament mit einem solchen Datenschutzauditzeichen.

Was ist zu tun?
Der Schleswig-Holsteinische Landtag kann als Vorbild für andere öffentliche Einrichtungen dienen, die Zutrittssysteme und Videoüberwachung einsetzen. Die Möglichkeit einer Auditierung sollte jeweils geprüft werden.

4 Datenschutz in der Verwaltung

4.1 Allgemeine Verwaltung

4.1.1 Der neue Personalausweis – ein Erfolgsmodell?

Der nPA ist da. Ob dessen elektronischer Identitätsnachweis im Alltag angenommen wird, muss sich noch zeigen. Die Perspektiven sind vielversprechend, der Aufwand, insbesondere für potenzielle Empfänger des Nachweises, ist allerdings beträchtlich. Das Verfahren der PIN-Vergabe durch die Meldebehörden ist noch nicht ausreichend abgesichert.



Den neuen Personalausweis (nPA) kann man als Quantensprung bezeichnen. Neben anderen Neuerungen wird erstmalig die Möglichkeit geschaffen, sich gegenüber privaten wie öffentlichen Stellen über das Internet online auszuweisen. Auf dem Ausweischip kann die qualifizierte digitale Signatur des Ausweisinhabers gespeichert werden. Selbst der Erwerb dieser Signatur ist durch die eID jetzt online möglich. Echte technische Sicherheitslücken haben sich beim **elektronischen Identitätsnachweis** (eID) – bis heute – nicht aufgetan. Allerdings setzt dessen sichere Nutzung eine gewisse Kenntnis der zugrunde liegenden Architektur sowie der notwendigen technischen Rahmenbedingungen voraus. So empfiehlt sich die Verwendung eines Chipkartenlesers mit eigener Zifferntastatur. Wer sich nicht genügend mit der Datensicherheit auskennt und die eID nicht dringend benötigt, sollte die eID besser deaktivieren lassen.

Ein **Sicherheitsrisiko** bei der eID sehen wir in der Möglichkeit, die Daten im Ausweischip über die Meldebehörde zu verändern, ohne dass ein Nachweis über die Änderung erfolgt. In der Papierversion muss jede Änderung von der Meldebehörde gesiegelt werden. Sie haftet so für die Richtigkeit der Änderung. Eine vergleichbare Dokumentation ist bisher in der elektronischen Form nicht vorgesehen, obwohl hier zusätzliche hochsensible Daten, insbesondere die PIN für die Freischaltung der eID, verändert werden können.

Im Alltag kommt es immer wieder vor, dass gültige Personalausweise bei örtlich unzuständigen Personalausweisbehörden abgegeben werden, sei es, dass sie verloren gegangen bzw. gestohlen und wiedergefunden wurden oder es sich um Ausweise Verstorbener handelt. Aktiviert nun ein Mitarbeiter der Behörde die eID und vergibt eine neue PIN, so kann dies zu einem massiven **Missbrauch der Funktion** führen. Eine Sperrung des Ausweises würde nicht stattfinden, wenn die eID ursprünglich nicht eingeschaltet war. Wird dann noch die Anschrift im Chip geändert, könnte bei einer unbefugten Nutzung der eID der potenzielle Vertragspartner unter Umständen nicht einmal auf den – falschen – Betroffenen schließen. Dieser würde die unbefugte Nutzung seiner eID nicht einmal bemerken. Fällt

dieser Missbrauch beim Vertragspartner auf, z. B. weil der Schuldner seine Forderung nicht begleicht, so würde auch eine Melderegisterauskunft nicht weiterhelfen, da durch die falsche Anschrift im Chip eine Ermittlung des Ausweisinhabers nicht möglich wäre. Nicht einmal die Sperrung des Ausweises wäre realisierbar, da das Sperrkennwort nicht ermittelt werden kann.

Weder die personalausweisrechtlichen Vorschriften noch die eingesetzte Technik sehen für den dargestellten Fall ausreichende Sicherheitsmaßnahmen bzw. eine ausreichende Revisionsfähigkeit der Datenverarbeitung vor. Bei mehr als 5.000 Personalausweisbehörden in Deutschland mit über 50.000 Mitarbeiterinnen und Mitarbeitern sehen wir hier dringenden **Nachbesserungsbedarf**. Um zumindest eine unbefugte Neusetzung der PIN in der Personalausweisbehörde zu verhindern, ist z. B. daran zu denken, zusätzlich zur Freischaltung die nur dem Betroffenen bekannte PUK mit einzugeben. Ist dies nicht möglich, muss im Zweifel die Sicherheit Vorrang haben und ein neuer Ausweis beantragt werden.

Bei den Meldebehörden in Schleswig-Holstein hat der nPA zu massiven Änderungen sowohl in **qualitativer wie in quantitativer Hinsicht** geführt. Die Zeiten, in denen lediglich Vordrucke ausgefüllt und in die EDV eingegeben wurden, sind endgültig vorbei. Der Bürger muss jetzt in technischer Hinsicht umfangreich beraten werden. Die Bearbeitung selbst basiert auf komplexer Technik und setzt ein entsprechendes Know-how der Mitarbeiter voraus. Die Bearbeitungszeiten haben sich – soweit bis heute erkennbar – massiv erhöht. Aus datenschutzrechtlicher Sicht ist es unsere vordringliche Aufgabe, durch Beratung und Hilfestellung zu einer Minimierung der Fehler beizutragen.

Was ist zu tun?
Die aufgezeigten Sicherheitsrisiken bei der PIN-Vergabe sollten von den dafür verantwortlichen Stellen durch geeignete konzeptionelle Änderungen beseitigt werden, bevor es zu tatsächlichen Missbräuchen der eID kommt.

4.1.2 Umgang mit ausgesonderten Datenträgern

Die Verwaltung muss immer wieder Hardware erneuern und dem Stand der Technik nicht mehr entsprechende Rechner aussondern. Was tun mit dem alten Kram?

Da hilft keine Flex, kein Hammer oder rohe Gewalt. Im Umgang mit alter Hardware sind besondere Grundsätze zu berücksichtigen. Diese darf nicht mit gespeicherten personenbezogenen Daten frei zugänglich sein oder z. B. auf einem Flohmarkt oder **Verkauf alter Gegenstände** an Technikliebhaber weitergegeben werden. Genau dies war in Glücksburg aber passiert, sodass plötzlich der Datenbestand der Kommune von mehreren Jahren für einen unberechtigten Dritten unverschlüsselt zur Verfügung stand.

Die Daten verarbeitende Stelle ist über den Zeitpunkt des Gebrauchs der Hardware hinaus für die von ihr erhobenen, verarbeiteten, genutzten und gespeicherten personenbezogenen Daten verantwortlich. Dies bedeutet, dass die personenbezo-

genen Daten dem Schutz des Landesdatenschutzgesetzes (LDSG) unterliegen und die Grundsätze der Datenschutzverordnung (DSVO) eingehalten werden müssen.

Was ist zu tun?
Die Verwaltung hat ihre alte Hardware auszusondern und muss die personenbezogenen Daten „wipen“, also nicht wiederherstellbar löschen. Eine Speicherung der personenbezogenen Daten über den Zeitpunkt der Erforderlichkeit der Datenverfügbarkeit hinaus ist nicht zulässig.

4.1.3 Datenschutzrechtliche Unterstützung bei der Ermittlung des Kindesvaters

Die Ermittlung des Vaters eines nicht ehelichen Kindes gestaltet sich für Jugendämter mitunter schwierig. Datenschutz darf solchen Ermittlungen grundsätzlich nicht im Wege stehen. In einem Fall führte ein Abgleich von Lichtbildern aus der Personalausweisdatei zwar nicht zum gewünschten Erfolg, aber immerhin zur Aufklärung des Sachverhaltes.

Über zwei Jahre lang ermittelte ein Jugendamt im Rahmen einer **Beistandschaft** nach dem Vater eines nicht ehelichen Kindes. Die Mutter hatte den Mann über das Internet kennengelernt. Nach einer kurzen Affäre riss der Kontakt ab. Die Mutter kannte nur den Vor- und Familiennamen, den Wohnort und das ungefähre Alter ihres Geliebten.

Eine entsprechende Melderegisteranfrage bei der zuständigen Stadt wurde abgelehnt, da der gesuchte Einwohner nach dem Melderecht nicht eindeutig **identifiziert** werden konnte. In Betracht kamen vier Personen, die mit gleichem Vor- und Familiennamen gemeldet waren. Eine weiter gehende „Listenanfrage“ hinsichtlich dieser Personen wurde ohne eine weitere Prüfung mit der gleichen Begründung abgelehnt. Nachforschungen über die Polizei und andere Stellen blieben erfolglos. Schließlich wandte sich das Jugendamt an uns mit der Bitte um Beratung ob aus unserer Sicht noch Möglichkeiten für Erfolg versprechende Nachforschungen bestehen.

Unsere Prüfung ergab, dass die **melderechtliche Listenauskunft** zu den vier in Betracht kommenden Personen fälschlicherweise verweigert wurde. Voraussetzung für eine solche Datenübermittlung ist, dass sie zur rechtmäßigen Aufgabenerfüllung der Behörde erforderlich ist. Da nur eine Person der Vater gewesen sein konnte, wären in drei Fällen Daten Nichtbetroffener übermittelt worden. Allerdings wäre der Eingriff in die Rechte dieser Nichtbetroffenen unter Verhältnismäßigkeitsgesichtspunkten deutlich geringer zu bewerten gewesen als die Gefahr, den Vater eines nicht ehelichen Kindes nicht ermitteln zu können.

Das Personalausweisgesetz eröffnete aber eine bessere datenschutzkonforme Lösung. Danach darf u. a. das gespeicherte **Lichtbild aus der Personalausweisdatei** übermittelt werden, wenn die ersuchende Behörde aufgrund von Rechtsvorschriften diese Daten erhalten darf, sie ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen und die Datenerhebung beim Betroffenen unverhältnismäßig wäre. Die bestehende Beistandschaft begründete

für das Jugendamt eine ausreichende Ermächtigung zur Datenerhebung. Bei einer Übermittlung der Meldedaten hätte eine persönliche Gegenüberstellung des Betroffenen mit der Mutter organisiert werden müssen. Wesentlich einfacher war es, der Mutter die Lichtbilder zu zeigen, ohne dabei weitere personenbezogene Daten der Kandidaten zu offenbaren. Die Mutter hätte so den Kindesvater identifizieren können, ohne dass die Betroffenen persönlich in Anspruch genommen werden mussten. Leider war der gesuchte Vater nicht unter den vorgelegten Kandidaten. Er hatte seinerzeit offensichtlich falsche Angaben gegenüber der Mutter gemacht. Das Verfahren hat dennoch zur Klärung des Sachverhaltes maßgeblich beigetragen und der Betroffenen zumindest die Gewissheit gebracht, dass nichts unversucht gelassen wurde.

4.1.4 Namentliche Nennung von Einwohnern in der Einwohnerfragestunde

Die Öffentlichkeit von Einwohnerfragestunden bedeutet nicht, dass Personen dort zwingend ihren Namen angeben müssen. Die Aufnahme in ein Protokoll, das im Internet veröffentlicht wird, darf nicht erfolgen, wenn der Bürger dies nicht wünscht.

Eine Amtsverwaltung wollte, dass bei Einwohnerfragestunden die Fragenden ihren Namen mitteilen. Dieser solle protokolliert und zusammen mit der Niederschrift über den Inhalt der Einwohnerfragestunde ins Internet eingestellt werden. Das ULD musste darauf hinweisen, dass es für die Veröffentlichung der Namen der Fragesteller **keine Rechtsgrundlage** gibt. Die Einwohnerfragestunde ist Teil der öffentlichen Sitzung der Gemeindevertretung. Die Gemeindeordnung sieht eine Niederschrift über jede Sitzung der Gemeindevertretung vor, bei der auch die Namen der Teilnehmerinnen und Teilnehmer aufzuführen sind. Dies betrifft jedoch lediglich die Gemeindevertreter, nicht die Bürger als Fragesteller.

Das Landesdatenschutzgesetz scheidet als Rechtsgrundlage für die Veröffentlichung aus; es fehlt bereits an deren Erforderlichkeit. Es geht lediglich darum sicherzustellen, dass als anfragende Personen nur **Einwohner der jeweiligen Kommune** Gehör finden. Um dies zu gewährleisten, genügt z. B. die Feststellung des Wohnsitzes durch Vorlage des Personalausweises. Nach einer solchen Verifikation ist keine weitere Datenverarbeitung mehr erforderlich. Es kommt insbesondere nicht darauf an, wer konkret welche Fragen stellt. Eine Erhebung und Veröffentlichung der Namen von Fragen stellenden Bürgern oder gar der Wohnanschrift im Internet ist daher nur zulässig, wenn die Betroffenen sich hiermit einverstanden erklärt haben.

Das ULD hat gemeinsam mit dem Innenministerium eine pragmatische Lösung gefunden. In der Praxis sind die meisten Fragesteller mit einer Veröffentlichung einverstanden. Zu Beginn der Sitzung weist der Vorsitzende der Gemeindevertretung oder eine sonst autorisierte Person darauf hin, dass Fragen, die von Einwohnern im Rahmen der Einwohnerfragestunde gestellt werden, namentlich protokolliert und die Protokolle im Internet veröffentlicht werden. Dabei ist ausdrücklich darauf hinzuweisen, dass die Betroffenen sofort oder auch später widersprechen können. **Widersprüche** sind umgehend zu berücksichtigen. Dies gilt auch bezüglich bereits veröffentlichter Protokolle. Diese sind so zu ändern, dass die Namen herausgenommen oder geschwärzt werden.

Was ist zu tun?
Die Vorsitzenden der Gemeindevertretungen müssen darauf achten, dass die Bürgerinnen und Bürger darüber aufgeklärt werden, dass der Protokollierung und Veröffentlichung ihrer Namen bei Einwohnerfragestunden widersprochen werden kann.

4.1.5 Zentrale Stellenbörse für die Landesverwaltung

Um den im Rahmen des Einsparkonzepts der Landesregierung beabsichtigten Stellenabbau zu unterstützen, soll im Finanzministerium eine zentrale Stellenbörse eingerichtet werden. Die notwendigen Befugnisgrundlagen für die Übermittlung sensibler Personalaktendaten durch die Ressorts konnten im Einvernehmen mit dem Finanzministerium datenschutzgerecht ausgestaltet werden.

Will man Personal einsparen, gilt es, Mitarbeiter, deren Stellen wegfallen sollen, ressortübergreifend schnell auf frei werdende Stellen zu versetzen, die wieder besetzt werden müssen. Für diese Aufgabe ist nach Auffassung der Landesregierung ein zentrales Personalmanagement unabdingbar. Dafür genügt es nicht, nur die Namen der in Betracht kommenden Mitarbeiter zu speichern. Nur mit einem **angemessenen Profil** kann die Koordinierungsstelle eine hinreichende Vorauswahl im elektronischen Verfahren vornehmen.

Da diese Aufgabe neu ist, war die für den Betrieb der Datenbank erforderliche Übermittlung von Personalaktendaten an die Koordinierungsstelle im Personaldatenrecht bisher nicht vorgesehen. Gemeinsam mit dem Finanzministerium haben wir eine Formulierung zur **Änderung des Landesbeamtengesetzes** gefunden, die die Datenübermittlung auf das tatsächlich notwendige Maß beschränkt und gleichzeitig eine umfassende Transparenz für die betroffenen Mitarbeiter sicherstellt. Da das Landesdatenschutzgesetz die Anwendung der beamtenrechtlichen Befugnisgrundlagen zur Datenverarbeitung auf alle Beschäftigten ausdehnt, ist eine gesonderte tarifvertragliche Regelung nicht erforderlich. Nach einer Ergänzung des Delegationserlasses des Ministerpräsidenten um die notwendige Zuständigkeitszuweisung für das Personalmanagement an das Finanzministerium steht einer Arbeitsaufnahme der Stellenbörse nichts mehr im Wege.

Aus unserer Sicht sichert die gefundene Lösung einen **angemessenen Ausgleich** zwischen den Interessen des Landes an einem effektiven Verfahren zur Unterstützung der beabsichtigten Personaleinsparungen und den Persönlichkeitsrechten der betroffenen Mitarbeiter.

4.1.6 Kosten- und Leistungsrechnung für EU-Projekte

Die finanzielle Förderung durch EU-Forschungsmittel im Bereich der Universitäten erfordert einen detaillierten Zeit- und Kostennachweis für die beteiligten Mitarbeiter. Da das Personalaktenrecht keine ausreichende Ermächtigung zur Weitergabe von Personaldaten an die EU enthält, kann die Lücke nur durch eine Dienstvereinbarung mit dem Personalrat geschlossen werden.

In der beabsichtigten Neuregelung des Beschäftigtendatenschutzes ist es ausdrücklich vorgesehen: „Andere Rechtsvorschriften im Sinne dieses Gesetzes sind auch Betriebs- und Dienstvereinbarungen." In diesem Sinne betrachten wir **Dienstvereinbarungen** mit dem Personalrat als ausreichende Ermächtigung zur Verarbeitung von Personaldaten, zumal das Personalaktenrecht insoweit keine abschließenden Regelungen enthält. Das Ministerium für Wissenschaft, Wirtschaft und Verkehr bat das ULD, beim Entwurf einer Musterdienstvereinbarung für eine Kosten- und Leistungsrechnung zur Abrechnung von Drittmittelprojekten behilflich zu sein.

Unsere Aufgabe bestand darin, die Anforderungen der EU und des Datenschutzes in Einklang zu bringen und gleichzeitig dafür zu sorgen, dass die beabsichtigte Personaldatenverarbeitung hinreichend präzise und für die Betroffenen **transparent** geregelt wird. In konstruktiver Zusammenarbeit mit dem Ministerium und Dataport als beteiligtem Projektentwickler konnten alle Knackpunkte einvernehmlich gelöst werden:

- Als Personal-Istkosten sollen nur die monatlichen **Bruttolohnsummen** der Mitarbeiter verwendet werden. Diese Beträge lassen keine Rückschlüsse auf einzelne Personalaktendaten der Mitarbeiter zu.
- Die Zeitabrechnung gegenüber dem Auftraggeber soll nur als Monatssumme je Mitarbeiter erfolgen. Die der Abrechnung zugrunde liegende interne **Zeitaufschreibung** soll als Tagessumme der geleisteten Stunden in einer von der Personalverwaltung getrennten Organisationseinheit erfolgen. Die Daten dürfen dort nur für Revisionszwecke verarbeitet werden.
- In den Abrechnungsunterlagen gegenüber dem Auftraggeber soll so weit wie möglich eine **Pseudonymisierung** der Personaldaten erfolgen.

Den Personalräten der Hochschulen blieb es natürlich unbenommen, den Entwurf der Musterdienstvereinbarung selbst zu bewerten und zusätzliche oder abweichende Bedingungen oder Beschränkungen aufzunehmen. Im Rahmen ihrer Beratungen haben sie sich allerdings unseren Hinweisen und Empfehlungen weitestgehend angeschlossen. Die notwendigen Dienstvereinbarungen wurden inzwischen abgeschlossen. Sie sehen angemessenen Ausgleich zwischen dem finanziellen Interesse des Landes am Erhalt von Drittmitteln zur Finanzierung von Forschungsvorhaben und den Datenschutzinteressen der betroffenen Mitarbeiter vor.

Was ist zu tun?
Die Musterdienstvereinbarung ist auf andere Bereiche des öffentlichen Sektors übertragbar.

4.1.7 Versand von Besoldungs- und Beihilfebescheiden im Bereich der Schulen

Die Praxis beim Versand von Besoldungs- und Beihilfebescheiden krankgeschriebener Mitarbeiter kann zu Missverständnissen und Irritationen führen. Der Versandweg sollte für die Betroffenen transparent und eindeutig nachvollziehbar sein.

Eine krankgeschriebene Lehrerin hatte mehrfach den Eindruck, an sie adressierte Bescheide des Finanzverwaltungsamtes seien auf dem Dienstweg vor der **Weiterleitung** an ihre Privatanschrift von der Schule geöffnet worden. Als Nachweis hatte sie einen entsprechenden Fensterbriefumschlag im Beisein eines Zeugen geöffnet und uns diesen anschließend übersandt. Der Umschlag war handschriftlich per Klebeetikett mit der Privatadresse der Betroffenen versehen worden und trug den Absenderstempel der Schule.

Der Schulleiter erklärte, die Bescheide vom Finanzverwaltungsamt würden per Dienstpost an die Schule gesandt. Sei der Betroffene erkrankt, werde der Brief keinesfalls geöffnet, sondern lediglich – wie dargestellt – um die fehlenden Angaben ergänzt und zur Post gegeben. Es bestand kein Anlass für Zweifel an den Aussagen des Schulleiters. Andererseits waren ein **Öffnen des Briefes** und die anschließende Verwendung eines neuen Umschlages unter Revisionsgesichtspunkten nicht völlig auszuschließen. Das praktizierte Verfahren hat bei der Mitarbeiterin und allgemein zu erheblichem Misstrauen und einem Vertrauensverlust gegenüber den Mitarbeitern der Schule geführt.

Vom Finanzverwaltungsamt erfuhren wir, dass Gehaltsmitteilungen über das Druckzentrum von Dataport als Dienstleister versandt werden. Briefe, die über dieses Druckzentrum verschickt werden, sind daran zu erkennen, dass sie im sogenannten **Nassklebeverfahren** verschlossen werden, weil nur so eine maschinelle Verarbeitung möglich ist. Üblich sind sonst heute nur noch Briefumschläge mit Selbstklebefolie als Verschluss. Bei der geprüften Schule waren nur noch Umschläge mit Selbstklebefolie im Einsatz. Da der vorgelegte Umschlag im Nassklebeverfahren verschlossen war, konnten wir eine Öffnung durch die Schule mit hoher Wahrscheinlichkeit ausschließen.

Was ist zu tun?
Um künftig ähnliche Fälle zu vermeiden, sollten Schulen bei längerer Erkrankung den Versand von Bescheiden durch das Finanzverwaltungsamt unmittelbar an die **Privatanschrift** der Betroffenen veranlassen. Ist dies nicht möglich, sollte der Originalbrief des Finanzverwaltungsamtes in einem zweiten Umschlag an die Betroffenen weitergeleitet werden, um Missverständnisse von vornherein zu vermeiden.

4.1.8 Einführung neuer elektronisch geführter Personenstandsregister

Die Einführung elektronisch geführter Personenstandsregister setzt neue Maßstäbe für die Verarbeitung personenbezogener Daten in einem landesweiten Verfahren. Da ein Nachweis der Daten in Papierform entfällt, sind höchste Sicherheitsstandards bei der Datenverarbeitung anzulegen. Die Vorschriften für die elektronische Registerführung legen in dieser Hinsicht präzise die notwendigen Details für die Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung fest.

Mit Verabschiedung des Personenstandsreformgesetzes im Jahr 2007 ist es amtlich: Die Personenstandsbücher haben ausgedient. Die Zukunft in den Standesämtern gehört den elektronischen Registern. Durch die Umstellung auf das elektronische Verfahren darf kein Qualitätsverlust im Hinblick auf die **Integrität und Vertraulichkeit** der gespeicherten Daten im Vergleich zu den bisherigen Personenstandsbüchern eintreten.

Bereits das Personenstandsgesetz trifft weitgehende Regelungen zur Datensicherheit. Die Identität der Person, die Eintragungen vornimmt, muss jederzeit erkennbar sein. Auswertungen des Registers müssen auf der Grundlage der aufzunehmenden Daten möglich sein. Die Sicherheitsanforderungen werden durch die Personenstandsverordnung präzisiert, die u. a. für Registereinträge eine dauerhaft überprüfbare **qualifizierte elektronische Signatur** des Standesbeamten vorschreibt. Außerdem werden umfangreiche Anforderungen an den Betrieb der elektronischen Register und die eingesetzten Datenverarbeitungsverfahren gestellt.

Das Innenministerium musste nun auf Landesebene für eine ordnungsgemäße Umsetzung der bundesrechtlichen Vorgaben sorgen. Dies geschah durch den Erlass einer **Landesverordnung** zur Einrichtung und Führung des zentralen elektronischen Personenstands- und Sicherungsregisters und durch Maßnahmen zur Organisation der zentralen Register bei Dataport als EDV-Dienstleister des Landes und der Kommunen.

Ein neuer Weg wurde für die auch in anderen Verfahren bereits aufgetretene Frage der Verantwortlichkeit für die Datenverarbeitung bei Dataport beschritten. Bisher waren die Kommunen als Daten verarbeitende Stellen ausschließlich hierfür zuständig. Sie mussten im Rahmen der **Auftragsdatenverarbeitung** als Auftraggeber gegenüber Dataport dafür sorgen, dass die Daten nur nach ihren Weisungen verarbeitet wurden. In einem landesweiten einheitlichen EDV-Verfahren mit über 160 beteiligten Kommunen hat aber eine einzelne Kommune nicht die Möglichkeit, eigenständige Anforderungen an die Organisation des Verfahrens bzw. an die Software zu stellen. Bei Dokumentation, Test und Freigabe ist es andererseits nicht notwendig, dass alle beteiligten Kommunen die gleichen umfangreichen Unterlagen vorhalten sowie dieselben Tests durchführen.

In der Landesverordnung wurde die Verantwortung für das bisher einheitliche Auftragsdatenverarbeitungsverhältnis aufgeteilt. Das Innenministerium als zuständige oberste Fachaufsichtsbehörde übernimmt danach die sogenannte **Verfahrensverantwortung** und ist damit zuständig für fachliche Vorgaben gegenüber

Dataport, für Test und Freigabe des Verfahrens sowie für die Kontrolle des rechtmäßigen Betriebs der Personenstandsregister. Bei den Kommunen verbleibt die sogenannte Datenverantwortung. Sie sind verantwortlich, dass die in den Registern gespeicherten Daten richtig und vollständig sind und im Rahmen der Konfiguration des Verfahrens vor Ort nur berechtigte Personen Zugang zu den Daten erhalten. Damit wurde erstmals eine **Lösung** für ein zentral betriebenes Verfahren gefunden, die die Verantwortlichkeit für die Datenverarbeitung praxisgerecht verteilt.

Was ist zu tun?
Bei landesweiten zentralen Verfahren sollte die Landesregierung ebenso wie bei ausschließlich elektronischer Datenverarbeitung, z. B. bei der melderechtlichen Spiegeldatenbank oder bei der elektronischen Personalakte, einheitliche Standards festlegen. Die Regelungen im Personenstandswesen haben insofern Vorbildcharakter, insbesondere bei der Organisation der Auftragsdatenverarbeitung.

4.1.9 Rabatte für Arzneimittel auch für Beihilfestellen

Durch das Arzneimittelrabattierungsgesetz können jetzt auch die Beihilfestellen des öffentlichen Dienstes Rabatte auf Arzneimittel erstattet bekommen, soweit sie entsprechende Beihilfeaufwendungen erbracht haben. Das notwendige Verwaltungsverfahren erfordert eine schnelle Anpassung der beamtenrechtlichen Beihilfevorschriften.

Ende 2010 wurde das „Gesetz zur Neuordnung des Arzneimittelmarktes in der gesetzlichen Krankenversicherung (AMNOG)“ verkündet. Darin wird der Kreis der berechtigten Stellen für Arzneimittelrabatte auf Unternehmen der privaten Krankenversicherung sowie die Träger der beamtenrechtlichen Beihilfe erweitert. Dieser Teil des Gesetzes wurde erst sehr spät in die parlamentarische Beratung eingebracht. Um kein Geld zu verschenken, ist bei den notwendigen Umsetzungsmaßnahmen **Eile geboten**.

Mit dem für das Beamtenrecht zuständigen Finanzministerium und dem Finanzverwaltungsamt bestand schnell Einvernehmen, dass für die zur Rabattierung notwendige Speicherung von Rezepten eine **Anpassung der Beihilfevorschriften im Landesbeamtengesetz** nötig ist. Noch zwischen den Feiertagen konnte ein Entwurf abgestimmt und auf den Weg gebracht werden, der hinsichtlich des Datenschutzes keine Wünsche offenlässt. Kernpunkte sind:

- Rezepte werden ohne Verknüpfung zum jeweiligen Beihilfevorgang ausschließlich zu **Revisionszwecken** höchstens ein Jahr lang elektronisch gespeichert.

- Eine Datenübermittlung an die sogenannte Zentrale Stelle bzw. den Treuhänder findet erst nach vollständiger **Anonymisierung** der Daten statt.

Was ist zu tun?
Nach zügiger Verabschiedung des Gesetzes ist dieses adäquat umzusetzen.

4.1.10 Solardachkataster sind datenschutzkonform möglich

Die Landeshauptstadt Kiel soll ein Solardachkataster erhalten. Nach entsprechender Beratung durch das ULD wird auf schutzwürdige Betroffeneninteressen geachtet.

Mit dem Ziel der Förderung CO_2-neutraler Energieerzeugung beschloss die Ratsversammlung der Landeshauptstadt die Einrichtung eines Solardachkatasters in Form eines Geoinformationssystems. Darin sollte der Eignungsgrad der Dachflächen in Kiel für die **solarenergetische Nutzung** dargestellt werden, auch als Entscheidungshilfe für Hauseigentümer bezüglich Investitionen in eine eigene Solaranlage.

Das Solarkataster basiert auf hochaufgelösten digitalen Oberflächenmodellen und Orthofotos – farbigen Luftbildern mit einer Bodenauflösung von 5 cm pro Pixel – sowie einer Stadtkarte in einem Maßstab von 1:10.000. Größe, Geometrie, Ausrichtung, Neigungswinkel und Verschattung der einzelnen Dachflächen sowie das minimale, maximale und mittlere Strahlungspotenzial werden erfasst, berechnet und dargestellt. Die Daten sind georeferenziert, also mit Raumkoordinaten verknüpft, sodass sie einem bestimmten Ort auf der Erdoberfläche zugeordnet und mit anderen ebenfalls georeferenzierten Informationen verschnitten, d. h. kombiniert werden können. Das individuelle **Solarenergieerzeugungspotenzial** jeder Dachfläche, also die Menge nutzbarer Strahlung je Gebäudedach, wird in einer Karte visualisiert. Auf den Internetseiten der Stadt Kiel soll über ein Webportal eine Übersicht sowie eine straßen- und hausnummergenaue digitale Karte mit Luftbildaufnahmen der Allgemeinheit zur Verfügung gestellt werden.

Die verarbeiteten Daten haben **Personenbezug**; Luftbilder wie auch die Angaben zu den Dachflächen lassen sich mit der Georeferenzierung ohne Weiteres den Eigentümern oder den an den jeweiligen Immobilien berechtigten Personen zuordnen. Mitgeteilt werden damit nicht nur Einspareffekte zugunsten der Umwelt, sondern auch das wirtschaftliche Potenzial des Einsatzes einer Solaranlage auf dem jeweiligen Dach und damit wirtschaftliche Möglichkeiten für die Betroffenen. Natürlich ist nicht auszuschließen, dass diese Daten z. B. für Werbezwecke genutzt werden.

Wegen Zweifeln an der Datenschutzkonformität der ursprünglichen Planung der Stadt Kiel seitens einiger Ratsmitglieder wurde das ULD um eine Bewertung gebeten. Wir mussten der Stadt mitteilen, dass ein einfacher Beschluss der Ratsversammlung als datenschutzrechtliche Rechtsgrundlage nicht ausreicht und praktische Änderungen nötig sind. Die Stadt Kiel erarbeitete, beraten vom ULD, als datenschutzrechtliche Rechtsgrundlage für das Kataster eine **Solardachkatastersatzung**. Dabei sind zwei verschiedene Versionen des Katasters vorgesehen. Eine interne Version basiert auf der Grundlage der im Einzelnen genannten Datenkategorien, welche die konkreten detaillierten Potenzialwerte für jede

Dachfläche individuell und hochauflösend enthält. Eine zweite, im Internet veröffentlichte Version stellt auf einer Stadtkarte mit dem Maßstab 1:10.000 die Dachflächen lediglich in Eignungsgraden eingestuft dar. Damit soll dem öffentlichen Interesse an einer allgemeinen Einschätzung des Potenzials für die Erzeugung von Solarenergie in Kiel Rechnung getragen werden, ohne dass die Betroffenen übermäßig in ihren Rechten beeinträchtigt werden. Das interne Kataster kann den Betroffenen Unterstützung bei der Entscheidung für die Installation einer Solaranlage bieten.

Um spezifischen Schutzbedürfnissen Einzelner und den Anforderungen des Landesdatenschutzgesetzes Rechnung zu tragen, sieht die Satzung ein **Widerspruchsrecht** vor. Eigentümerinnen und Eigentümer oder anderweitige Rechteinhaber können gegen die Veröffentlichung Widerspruch erheben mit der Folge, dass die Darstellung der jeweiligen Dachflächen unterbleibt oder nachträglich entfernt wird. Um dieses Recht rechtzeitig wahrnehmen zu können, muss die Stadt die Öffentlichkeit sechs Wochen vor der Webpräsentation über das Solardachkataster und das Widerspruchsrecht in der Lokalpresse informieren.

Was ist zu tun?
Bei der Entwicklung und dem Einsatz von Geoinformationssystemen müssen die verantwortlichen Stellen Datenschutzbelange frühzeitig in die Planung einbeziehen und die notwendigen rechtlichen, organisatorischen und technischen Maßnahmen ergreifen, um die Verletzung der Persönlichkeitsrechte auszuschließen.

4.2 Polizei und Verfassungsschutz

Im **Spannungsverhältnis** zwischen den Zielen des Grundrechtsschutzes und der Gewährleistung von Sicherheit steht derzeit die Auseinandersetzung um die Vorratsspeicherung von Telekommunikationsverkehrsdaten zu Zwecken der Bekämpfung von Kriminalität im Internet (Tz. 2.4). Dies ist aber beileibe nicht die einzige datenschutzrechtliche Baustelle, an der gearbeitet wird. Das Bundesverfassungsgericht befasst sich mit dem Bundeskriminalamtgesetz (Tz. 4.2.10). Auf europäischer Ebene findet eine intensive Diskussion über den Datenaustausch zwischen Sicherheitsbehörden in der EU und den USA statt.

Neben Fragen der Regulierung befasst sich das ULD mit konkreten und allgemeinen Themen der Praxis. Dabei bleibt die Erneuerung der **Informationstechnik der Sicherheitsbehörden** auf Landes- und auf Bundesebene ein Dauerbrenner. Während im Land Datenschützer und Polizisten gemeinsam nach Lösungen suchen (Tz. 4.2.2), hat sich am Kommunikationsdefizit auf Bundesebene nichts geändert. An den Datenschützern liegt es dabei nicht (Tz. 4.2.6 und Tz. 4.2.8).

Ein Beispiel, wie Belange des Persönlichkeitsschutzes und der Sicherheit weitgehend in Einklang gebracht werden können, ist die Entwicklung moderner **Körperscanner**, mit denen insbesondere bei Flughafenkontrollen gefährliche Gegenstände und Waffen erkannt werden sollen. Mit Terahertzstrahlung, die von der menschlichen Haut reflektiert wird, werden dabei bekleidete Menschen

durchleuchtet. Die dabei entstehenden Bilder stellen die Menschen nackt dar, was heikle moralische und rechtliche Fragen auslöst. Das ULD wurde vom Bundesbildungsministerium um ein Gutachten gebeten, wie die Personenkontrollen datenschutzkonform möglich gemacht werden können. Die Bundespolizei entwickelte daraufhin in Lübeck Geräte, die die kontrollierten Personen nicht mehr nackt, sondern nur abstrahiert darstellen, aber auf mögliche Gefahrenquellen hinweisen. Diese sind inzwischen auf dem Flughafen in Hamburg im Probebetrieb.


https://www.datenschutzzentrum.de/sicherheitstechnik/20100331-koerperscanner.html

4.2.1 Jugend-Taskforce zur Bekämpfung von Jugendkriminalität

Die Landesregierung hat eine Arbeitsgruppe eingerichtet, die im Auftrag des Landtages Vorschläge erarbeitet, wie der Entstehung und der Ausübung von Jugendkriminalität entgegengewirkt werden kann. Das ULD ist in der Arbeitsgruppe vertreten.

Die Arbeitsgruppe befasst sich mit der Präventionsarbeit für Jugendliche sowie mit der Zusammenarbeit all der Stellen, die Jugendliche betreuen oder sich mit Jugendkriminalität beschäftigen, z. B. Schule, Jugendamt, Polizei, Staatsanwaltschaft oder Gericht. Die bei den unterschiedlichen Stellen vorhandenen, oftmals sensiblen Informationen über auffällige oder bereits straffällig gewordene Jugendliche sollen ausgetauscht werden, um aufeinander abgestimmte Erfolg versprechende Maßnahmen zu treffen. Ist für eine Zusammenarbeit und Abstimmung mehrerer Stellen die Nennung des betroffenen Jugendlichen nicht erforderlich, so genügt der Austausch anonymisierter Daten. Sind Rückschlüsse auf den betroffenen Jugendlichen nicht möglich, ist der Austausch datenschutzrechtlich kein Problem. Dies genügt in einigen Fällen jedoch nicht, z. B. wenn zwischen Stellen mit Kontakt zu dem betroffenen Jugendlichen konkrete Lösungen für den weiteren Umgang mit dem Heranwachsenden abgestimmt werden sollen. Dies setzt **Datenübermittlungen** voraus, die jeweils entweder durch eine gesetzliche Befugnis oder durch eine Einwilligung des betroffenen Jugendlichen erlaubt sein müssen. Ein erster Zwischenbericht der Arbeitsgruppe befasst sich auch mit einer vom ULD beigesteuerten ausführlichen Darstellung und Erläuterung der datenschutzrechtlichen Anforderungen beim Informationsaustausch. Der Bericht (LT-Drs. 17/665) ist abrufbar unter:


http://www.landtag.ltsh.de/infothek/wahl17/drucks/0600.html

Die Arbeitsgruppe prüft nun auch die Frage, ob die bestehenden **Befugnisse ausreichend** sind, um den notwendigen Informationsaustausch zwischen Behörden abzudecken. Die Ergebnisse werden in einem zweiten Berichtsteil voraussichtlich Anfang 2011 veröffentlicht.

4.2.2 Das Verfahren @rtus

Bei dem vor mehr als fünf Jahren als Vorgangsbearbeitungssystem der Polizei des Landes gestarteten System @rtus-VBS ist es Zeit für einen ersten Blick auf die Qualität der gespeicherten Daten des Verfahrens insgesamt, zumal neue IT-Verfahren entwickelt werden, die auf dem Bestand des Vorgangsbearbeitungssystems beruhen.

Die Datenqualität von @rtus-VBS

@rtus ist ein komplexes Verfahren zur Unterstützung der Polizei bei deren täglicher Arbeit. In @rtus werden z. B. Anzeigen oder sonstiger Schriftverkehr, der im Laufe der Bearbeitung eines Vorgangs anfällt, erfasst. @rtus, so eine Zielvorgabe, soll das **Tor in eine papierlose Welt** eröffnen. Bei einem Verfahren, das künftig ohne Akten auskommen soll, kommt es besonders auf die Validität der gespeicherten Daten an. In Akten werden neben den Maßnahmen der Polizei weitere Informationen zum Nachweis der Rechtmäßigkeit des polizeilichen Handelns festgehalten. Der Verlässlichkeit und Richtigkeit der Daten kommt enorme Bedeutung zu; die Polizei hat hieran ein fachliches Eigeninteresse und muss hierauf ein besonderes Augenmerk legen. Der Betroffene kann nur im Ausnahmefall, nämlich wenn er Kenntnis von den gespeicherten Daten hat, unrichtige Datenspeicherungen berichtigen lassen. Gesetzeskonforme Datenverarbeitung bedingt eine hohe gesicherte Datenqualität.



Das ULD prüfte anlässlich einer Eingabe die Datenspeicherungen von neun Personen in @rtus. Dabei ergaben sich Zweifel hinsichtlich **Richtigkeit und Logik** der Speicherungen. Manches war selbst für Polizeibeamte nicht ohne Weiteres nachvollziehbar. Gute Datenverarbeitung muss „selbstsprechend" sein und jedem berechtigten polizeilichen Anwender richtige und verlässliche Daten zur Aufgabenerfüllung bereitstellen. Ist dies nicht der Fall, werden den gewünschten Workflow beeinträchtigende Rückfragen nötig. Durch dauernde Qualitätssicherung lassen sich solche Mängel vermeiden. Diese gehört nicht nur bei Unternehmen der Wirtschaft, sondern auch bei vielen Behörden heute zum Standard. Datenqualität ist Gradmesser für die Effektivität und gibt Auskunft über die Effizienz von Verfahren, was mit Blick auf die Finanzlage des Landes immer mehr an Bedeutung gewinnt.

Die multifunktionale Datenbasis

Die Daten aus @rtus-VBS sollen nach polizeilichen Planungen weitere Verwendungen finden. Worüber während der Konzeption und Realisierung des Vorgangsbearbeitungssystems nicht konkret gesprochen wurde, ist inzwischen fast

selbstverständlich geworden, was die gesetzlich auferlegten Restriktionen bezüglich der zweckbestimmten Verarbeitung in einem neuen Licht erscheinen lässt. Die Zwecke der Vorgangsbearbeitung und der Dokumentation wurden bislang restriktiv interpretiert. Jetzt soll eine neue Sichtweise her. In Gesprächen mit Polizei und Innenministerium kam das ULD zu dem Ergebnis, dass weitere Nutzungen des @rtus-VBS-Datenbestandes unter dem Aspekt der rechtlichen Erforderlichkeit zur Aufgabenerfüllung möglich sind. Dabei geht es z. B. um elektronische **Zusammenstellungen und Auswertungen**, die bisher in mühevoller Kleinarbeit „händisch“ erfolgten. Die Vorteile des neuen Vorgehens liegen nicht nur ökonomisch in der Einsparung von Ressourcen und in besseren Arbeitsabläufen, sondern auch datenschutzrechtlich in einem verlässlichen Datenbestand und einem kontrollierten sicheren Verfahren. Stellt sich jedoch heraus, dass die Datenbasis nicht verlässlich ist, so muss sich das ULD wegen der drohenden Datenschutzeinbußen gegen eine weitere Verwendung der Daten und somit gegen neue Anschlussprojekte von @rtus aussprechen.

@rtus-Recherche – ein neues Verfahren

Das ULD wurde von der im Landeskriminalamt (LKA) eingerichteten Projektgruppe „@rtus-Auswertung“ frühzeitig bei der Konzeptionierung des neuen Verfahrens „@rtus-Recherche“ beteiligt. Dabei geht es um **differenzierte Recherchemöglichkeiten** für mit Ermittlungen beauftragte Polizeibeamte, für kriminologische Phänomenbereiche bearbeitende LKA-Experten und für wenige LKA-„Super-User“, die ausschließlich spezielle tief gehende Recherchen bearbeiten. Die Projektgruppe präsentierte Konzepte, die abhängig von der Art der Recherche und von der Gruppe der Nutzer modifizierte Leserechte auf den Datenbestand vorsehen. Der „normale“ Ermittlungsbeamte kann im Rahmen der ihm zugestandenen Recherche nur die Vorgänge seiner Dienststelle und die Vorgangsrumpfdaten fremder Polizeidienststellen sehen. Dem Super-User im LKA, der sehr spezielle Recherchen durchführen kann, stehen künftig Auswertetools zur Verfügung, die einen Blick auf den Gesamtdatenbestand erlauben. Der LKA-Experte erhält einen Datenzugriff zwischen dem des Ermittlungsbeamten und dem des Super-Users.

Unter dem Aspekt, dass die Polizei im Rahmen der rechtlichen Grenzen ihren Datenbestand effektiv nutzen können muss, haben wir keine grundlegenden Bedenken erhoben. Doch forderten wir neben einer umfassenden Protokollierung eine Qualitätsprüfung der Daten aus @rtus-VBS, die Grundlage der Recherchen sind, hinsichtlich Geeignetheit und Erforderlichkeit. Für diese Prüfung sollte die Polizei ein technisches Verfahren entwickeln, das sich z. B. an den den jeweiligen Sachverhalt erfassenden Strafnormen orientiert und das über einen Straftatenkatalog pauschalierte Zuordnungen zulässt. Die Relevanz der Datensätze für den eigenen Recherchezweck muss vom Sachbearbeiter im Einzelfall beurteilt werden. Der mit der **Relevanzprüfung** verbundene Aufwand ist vertretbar und auch im Interesse des Grundrechtsschutzes angemessen.

Wir forderten weiterhin die Festlegung gesetzeskonformer **Aussonderungsprüffristen** im Rahmen einer dreijährigen Evaluierung. Die bisherige Frist nach der Errichtungsanordnung beträgt in der überwiegenden Zahl der Fälle bis zu fünf

Jahren. Zur Vermeidung von Fristüberschreitungen sind wir mit dem Innenministerium und der Polizei übereingekommen, dass für die Dauer der Evaluierung eine dreijährige Aussonderungsprüffrist gelten soll.

Konstruktive Kooperation bei Entwicklung von Data-Warehouse-Konzepten

Data Warehouse ist in der modernen Informationstechnik längst kein Zauberwort mehr. So verwundert es nicht, dass die Polizei bei neuen Verfahren diese Art der Informationsverarbeitung einsetzt. Ein Datenbestand steht für die Verarbeitung für verschiedene Zwecke bereit und kann entsprechend den polizeilichen Bedürfnissen genutzt werden. Die Projektgruppe „@rtus-Auswertung" erkannte frühzeitig, dass das Konzept eines Data Warehouse besondere Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung mit sich bringen kann. In einer kleinen **Arbeitsgruppe** unter Beteiligung des Innenministeriums und des ULD wird dies näher untersucht. Beteiligt sind zudem Teilnehmer aus dem Projekt „@rtus-Auswertung", vom Dienstleister Dataport und für die Polizei Schleswig-Holstein tätige Softwareentwickler. Aus Sicht der Arbeitsgruppe sind technische Lösungen für den Einsatz eines Data Warehouse auf der Basis der bestehenden Gesetze realisierbar. Die Arbeitsgruppe legt ihren Abschlussbericht nach Fertigstellung dem Innenministerium, dem Landeskriminalamt und dem Landespolizeiamt vor.

Ziele der Arbeitsgruppe sind es,

- die funktionalen Anforderungen an den Einsatz eines Data Warehouse bei der Polizei des Landes Schleswig-Holstein zusammenzufassen,
- die Bedarfsträger zu benennen,
- einzelne Nutzungsszenarien darzustellen,
- in zwei konkret benannten Lageszenarien die Anforderungen zu formulieren und
- einen Ausblick auf kommende Anforderungen zu wagen.

Das ULD will mit diesen Ergebnissen eine **Diskussion mit den Datenschutzbeauftragten** des Bundes und der Länder starten. Auch bei den anderen Polizeibehörden in Deutschland werden zunehmend Data-Warehouse-Verfahren eingesetzt.

Was ist zu tun?
Die Polizei ist gut beraten, auf gesicherte und richtige Daten in @rtus zu achten und selbstkritisch kontinuierliche Kontrollen durchzuführen.

4.2.3 Dokumentation von Datenübermittlungen

Datenübermittlungen der Polizei sind nach dem Willen des Gesetzgebers in den Akten zu dokumentieren.

Ein Petent beschwerte sich beim ULD, dass eine Kopie des Protokolls der von der Polizei vorgenommenen **Durchsuchung seiner Wohnung** bei einer ARGE gelandet sei. Dies sei nicht zulässig, da er Rente beziehe und keine Leistungen der ARGE. Das Verfahren der Polizei richtete sich gegen ihn wegen des Verdachts des Sozialleistungsbetruges. Es wurde eingestellt. Die teilweise aus der Durchsuchung stammenden polizeilichen Erkenntnisse waren tatsächlich an die ARGE weitergegeben worden. Eine Datenübermittlung der Polizei an die ARGE war insoweit rechtens, wie diese zur Begründung eines Anfangsverdachts der Erschleichung von Sozialleistungen durch die Lebensgefährtin des Petenten erforderlich war. Nur war im Rahmen unserer Kontrolle nicht mehr zu klären, welche Daten konkret an die ARGE übermittelt wurden, da sich hierüber kein Nachweis in den polizeilichen Unterlagen befand. Die Weitergabe des Durchsuchungsprotokolls an die ARGE war nicht erforderlich, es enthielt keine Angaben zur Begründung eines Anfangsverdachts. Wir beanstandeten, dass die Datenübermittlung nicht korrekt ausgewiesen wurde; zudem rügten wir die Übermittlung des Protokolls der Wohnungsdurchsuchung.

Das Innenministerium nahm sich des Falles an und konnte feststellen, dass der Übermittlungsnachweis in der **Akte der Staatsanwaltschaft** enthalten war. Doch hätte die Daten verarbeitende Stelle bei der Polizei den Nachweis zum Zeitpunkt der Kontrolle selbst erbringen müssen.

Was ist zu tun?
Die Polizei muss ihre Datenverarbeitung in Akten oder Dateien so organisieren, dass sie jederzeit erfolgte Übermittlungen und möglichst auch deren Inhalt nachweisen kann. Dies dient nicht nur datenschutzrechtlichen Kontrollen, sondern auch zur Realisierung gesetzlich vorgesehener Nachberichtspflichten.

4.2.4 Protokollierung – ein offenbar unlösbares Problem

In der Privatwirtschaft wie bei anderen Polizeien, etwa beim Bundeskriminalamt, geht der Trend zur vollständigen Protokollierung der Transaktionen in IT-Verfahren. Die Polizei pocht dagegen weiter auf ihre lückenhafte Protokollierung.

Das ULD bemüht sich seit geraumer Zeit die Polizei zu bewegen, die Protokollierung aller Abrufe aus ihren Dateien vorzusehen (32. TB, Tz. 4.2.5). Dies gehört heutzutage zum allgemeinen Standard der Datensicherheit und liegt im ureigenen Interesse der verantwortlichen Stelle. Doch eine solche Sicherheit ist für die Polizei in Schleswig-Holstein offenbar tabu. Wer die Protokollierung bei **bestimmten Personengruppen** ausschließt, weil immer ein berechtigter lesender Zugriff auf die Daten unterstellt wird, läuft Gefahr, dass Fälle des Datenmissbrauchs nicht

aufgeklärt werden können. Alle Weiterentwicklungen des Verfahrens @rtus leiden an diesem nicht hinnehmbaren Mangel.

Was ist zu tun?
Die Polizei des Landes sollte endlich anerkannte Standards der Datensicherheit akzeptieren und bei den eigenen Verfahren einsetzen. Notfalls ist der Gesetzgeber aufgerufen, hier für eine klare verpflichtende Regelung im Landesverwaltungsgesetz zu sorgen.

4.2.5 Falsch verbunden? Mobilfunknotrufe 112 und die Polizei

Notrufe von Mobiltelefonen an die Notrufnummer 112 wurden in der Vergangenheit an die Leitstellen der Polizei geleitet, dort angenommen und an die Rettungsleitstellen weitergeleitet. Mit der Einführung der neuen Leitstellen in Schleswig-Holstein findet diese Praxis endlich ein Ende.

Mit Inkrafttreten der Verordnung des Bundes über Notrufverbindungen im Jahr 2009 wurde die Rufnummer 110 neben der bestehenden Notrufnummer 112 als zusätzliche nationale Notrufnummer festgelegt. Zuvor waren Telefonanbieter nicht verpflichtet, die „110“ ebenso vorrangig zu behandeln wie die „112“. Das führte für Notrufe aus dem Mobilfunknetz dazu, dass Notrufe an beide Nummern **gebündelt an die Polizeileitstellen** geroutet wurden. Damit erlangt die Polizei von Rettungsnotrufen und damit zusammenhängenden Sachverhalten Kenntnis, die nicht für sie bestimmt und die für ihre Aufgabenerfüllung nicht erforderlich sind. Ergeben sich aus einer Notfallsituation so Hinweise auf eine Straftat, z. B. bei einer Überdosierung von Rauschmitteln, kann die Polizei durch die Entgegennahme des Notrufs auch hiervon erfahren und aufgrund des Legalitätsprinzips zur Aufnahme von Ermittlungen verpflichtet sein, obwohl der Anrufer dies weder erwartet noch gewollt hat.

Das Ministerium für Arbeit, Soziales und Gesundheit teilte nun mit, dass das Routing für Notrufe aus dem Mobilfunknetz im Zuge der **Einführung der neuen Leitstellen** in Schleswig-Holstein geändert wird. In den neuen Leitstellen Nord, West und Mitte kommen die Notrufe aus dem Mobilfunknetz direkt bei der Rettungsleitstelle an.

Was ist zu tun?
Der Umstellungsprozess muss schleunigst fortgeführt und abgeschlossen werden, damit Notrufe ohne Umweg den richtigen Adressaten erreichen.

4.2.6 INPOL-Arbeitsgruppe der Datenschützer – ohne Chancen?

Seit vielen Jahren bemühen sich die Datenschutzbeauftragten, die Polizeien des Bundes und der Länder bei der Weiterentwicklung des Informationssystems der Polizei (INPOL) in Datenschutzfragen zu beraten.

Die Zusammenarbeit gestaltet sich äußerst schwierig, weil die Datenschutzbeauftragten **nicht ausreichend informiert** und beteiligt werden. Der Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wandte sich deshalb an den Bundesminister des Innern und an die Konferenz der Innenminister (AK II). Die Antwort des Bundesinnenministers war desillusionierend und lässt nicht erkennen, dass die bestehende Praxis geändert werden soll. Der AK II zog es bisher vor, nicht zu antworten.

Die Tätigkeit der Datenschutzbeauftragten dient einer dauernden **projektbegleitenden Beratung** und Diskussion der bei dem Projekt auftretenden Datenschutzfragen. In den vergangenen Jahren drohte dieser Ansatz aufgrund der Minimalinformationen durch das BKA zu einer Alibiveranstaltung zu degenerieren. Ein bis zwei Treffen jährlich, die jeweils ca. zwei Stunden dauerten, und vereinzelte Konzepte zu Dateien sind die Informationsbasis. Eine adäquate Betrachtung des Gesamtvorhabens und der einzelnen Dateien ist so nicht zu leisten.

Die Datenschutzbeauftragten fordern weiterhin von der Projektgruppe INPOL im BKA die Übersendung zahlreicher Unterlagen sowie Sachstandinformationen. Den Datenschutzbeauftragten ist daran gelegen, ihren gesetzlichen Beratungsauftrag bestmöglich zu erfüllen; die beteiligten Sicherheitsbehörden zeigen weiterhin ungenügendes Interesse am Datenschutz. Dadurch drohen gewaltige **Fehlinvestitionen**. INPOL-neu wird die Informationsverarbeitung der deutschen Polizei auf längere Zeit prägen und dominieren. Eine datenschutzkonforme Gestaltung müsste gemeinsames Anliegen von Polizei und Datenschutz sein. Was im Land Schleswig-Holstein möglich ist, sollte auf Bundesebene für die Kooperation mit der PG-INPOL im BKA auch machbar sein (Tz. 4.2.2).

Was ist zu tun?
Der Bundesinnenminister und die Projektgruppe INPOL im BKA müssen sich für eine konstruktive Zusammenarbeit mit den Datenschützern entscheiden.

4.2.7 Volltextrecherche bei Sicherheitsbehörden − ein Paradigmenwechsel

Moderne Datenbanken und Data-Warehouse-Verfahren erlauben es den Anwendern, ohne großen Mehraufwand Textdokumente zu Personen zu speichern und die Texte Wort für Wort auszuwerten.

Die neue Qualität der modernen Datenverarbeitung hinterlässt im Recht der Sicherheitsbehörden tiefe Spuren. Angaben über Personen, die eigentlich nicht im Visier der Verfassungsschutz- oder Polizeibehörde stehen, werden gespeichert und sind zu recherchieren. Der Kreis der rechtmäßig Erfassten wird um eine

unbestimmte Zahl weiterer Personen erweitert, die aus irgendeinem Anlass im Zusammenhang mit einer Zielperson in einem Dokument genannt sind. Gesetzliche Regelungen, die eine abschließende Aufzählung der Kategorien von Daten zu bestimmten Personen vorsehen, werden so unterlaufen. Die Auswirkungen für die Betroffenen können in der Praxis erheblich sein und zu beträchtlichen Nachteilen führen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu eine Entschließung gefasst, die im Internet abrufbar ist unter:



http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/80DSK_VolltextsucheSicherheitsbeh%C3%B6rden.pdf?__blob=publicationFile

4.2.8 NADIS-neu – Datenschützer auch hier nicht erwünscht

Das gemeinsame Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder, NADIS, wird mit hohem finanziellen und technischen Aufwand neu gestaltet. Es soll im nächsten Jahr in Wirkbetrieb gehen. Die Umsetzung des Datenschutzes beim neuen Verfahren ist ein selbst vor Datenschützern gehütetes Geheimnis.

Die Verfassungsschutzbehörden haben sich unter Federführung des Bundesamtes für Verfassungsschutz (BfV) vor einigen Jahren zur Aufgabe gemacht, das technisch veraltete NADIS durch ein zeitgemäßes Verfahren zu ersetzen, das auch künftigen fachlichen Anpassungen, z. B. Änderung von rechtlichen Grundlagen, ohne größeren Aufwand gerecht werden kann (32. TB, Tz. 4.2.7). Vorgesehen sind neben der technischen Erneuerung des Verfahrens auch die Einbeziehung von **Multimediadaten und Textdokumenten**, was zu einer massiven Erweiterung führt. Die beliebige Recherche in Volltextdateien bei Sicherheitsbehörden ist generell rechtlich problematisch, insbesondere bei den Nachrichtendiensten (Tz. 4.2.7).

In einer beim BfV angesiedelten Projektgruppe arbeiten alle Verfassungsschutzbehörden an der Neugestaltung von NADIS. Die Datenschutzbeauftragten des Bundes und der Länder bieten in Fragen des Datenschutzes ihre **begleitende Beratung** an. Der Staatssekretär im Bundesinnenministerium (BMI) meinte jedoch, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) vom BfV durch Bereitstellung von Dokumenten und gemeinsame Besprechungen genügend eingebunden werde. Die Kommunikation zwischen Landesverfassungsschutz und Landesdatenschutz solle auf Länderebene erfolgen – bei einem bundesweiten Verbundprojekt!

Die Leitungen der Verfassungsschutzbehörden befürworteten einstimmig, dass der Arbeitskreis Sicherheit der Datenschutzbeauftragten des Bundes und der Länder regelmäßig durch die Projektgruppe NADIS-neu informiert wird. Diese Information der Landesdatenschutzbeauftragten erfolgte bisher aber nur auf den zweimal jährlich stattfindenden Sitzungen des Arbeitskreises Sicherheit, wo der BfDI **lediglich in sehr allgemeiner Form** über das Projekt unterrichten kann, da das BMI bzw. das BfV einer konkreten Weitergabe der Informationen bzw. Unterlagen an die Landesdatenschutzbeauftragten nicht zugestimmt hat. Der

Leiter der Verfassungsschutzbehörde des Landes hat sich auf Bitten des ULD bereit erklärt, auf Bundesebene auf eine bessere Einbindung der Landesdatenschutzbeauftragten zu drängen. Bisher erfolgt keine angemessene Information über NADIS-neu. Es geht um ein kostspieliges Projekt zur Verarbeitung hochsensibler Daten. Gesetzes- und datenschutzwidrige Fehlplanungen sollten dringend vermieden werden.

Das **Verfassungsschutzgesetz Schleswig-Holstein** enthält abweichende Regelungen zu den Verfassungsschutzgesetzen des Bundes und anderer Länder. Bei der technischen Einbindung des Landes in die IT-Landschaft des Verfassungsschutzes muss dem Rechnung getragen werden.

Was ist zu tun?
Das Bundesinnenministerium lässt bisher keine Bereitschaft zu einem konstruktiven Dialog erkennen. BMI und die Verfassungsschutzbehörden sollten ihre Verweigerungshaltung aufgeben. Eine Beteiligung der Datenschutzbehörden der Länder brächte auch ihnen einen Gewinn.

4.2.9 Videoüberwachung öffentlicher Plätze

Zur Reduzierung von Gefahren und Straftaten an Kriminalitätsbrennpunkten setzen immer mehr Städte und Gemeinden auf Videoüberwachung.

Das Landesverwaltungsgesetz erlaubt die Videoüberwachung öffentlicher Plätze, wenn es sich um Kriminalitäts- oder Gefahrenschwerpunkte handelt und Tatsachen die Annahme rechtfertigen, dass auch in Zukunft dort Schäden für Leib, Leben oder Freiheit oder gleichgewichtige Schäden für andere Rechtsgüter zu erwarten sind. Die Maßnahme ist auf sechs Monate zu befristen. Angefertigte Aufnahmen sind nach spätestens einem Monat zu löschen. Von dieser Regelung wird in Schleswig-Holstein im Einzelfall Gebrauch gemacht, einige Kommunen erwägen den Einsatz von Videoüberwachung und baten das ULD um Beratung. Sie arbeiten dabei oftmals eng mit der Polizei zusammen. Verantwortlich für die Beschaffung, die Einrichtung und den Betrieb der Anlage ist zumeist die kommunale Ordnungsbehörde. Die Bilder der Kamera werden regelmäßig an die Polizei übertragen, die im konkreten Gefahrenfall als Gefahrenabwehrbehörde tätig wird. Auch die Aufzeichnungen werden bei der Polizei gespeichert, da diese im Regelfall nur für

Im Wortlaut: § 184 Abs. 2 LVwG

Allgemein zugängliche Flächen und Räume dürfen mittels Bildübertragung beobachtet werden, soweit dies zur Aufgabenerfüllung nach § 162 erforderlich ist. Der offene Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder Bildaufzeichnungen in und an allgemein zugänglichen Flächen und Räumen, die Kriminalitäts- oder Gefahrenschwerpunkte sind, ist zulässig, soweit Tatsachen die Annahme rechtfertigen, dass Schäden für Leib, Leben oder Freiheit oder gleichgewichtige Schäden für andere Rechtsgüter zu erwarten sind. Die Maßnahme nach Satz 2 ist örtlich auf den erforderlichen Bereich zu beschränken und auf sechs Monate zu befristen. Eine Verlängerung ist nur zulässig, sofern die Voraussetzungen nach Satz 2 weiterhin vorliegen.

Zwecke der Strafverfolgung relevant sind. Das ULD hat eine **Checkliste** als Hilfe für die Entscheidung über die Einrichtung einer Videoüberwachungsanlage veröffentlicht unter:



https://www.datenschutzzentrum.de/video/checkliste.html

Zu beachten sind insbesondere folgende Anforderungen:

- Bei dem zu überwachenden Platz muss es sich um einen Kriminalitäts- oder Gefahrenschwerpunkt handeln. Es muss dort zu einer signifikanten Häufung von Straftaten oder Gefahren kommen; diese muss durch entsprechende Zahlen belegt sein. Ein subjektives Empfinden der Bevölkerung genügt nicht. Es müssen Schäden für Leib, Leben oder Freiheit oder gleichgewichtige Schäden für andere Rechtsgüter zu erwarten sein. Das Eigentum ist als Rechtsgut nicht ausdrücklich genannt. Zum Schutz des Eigentums ist die Maßnahme nur zulässig, wenn gewichtige Schäden zu erwarten sind.
- Die Videoüberwachung dient der Gefahrenabwehr. Die Möglichkeit, Aufzeichnungen für die Strafverfolgung zu nutzen, ist nur ein zulässiger Nebenzweck. Die Videoüberwachung muss also in erster Linie zur Gefahrenabwehr geeignet sein. Dies setzt voraus, dass den betroffenen Bürgerinnen und Bürgern in einer tatsächlichen Gefahrensituation durch die Maßnahme geholfen werden kann, was eine Liveübertragung der Bilder verlangt. Mit dem bloßen Aufzeichnen der Bilder kann zwar eine nachträgliche Untersuchung von Vorfällen erfolgen, nicht aber die Abwehr von Gefahren.
- Die Übertragung der Bilder von der Kamera zu dem Überwachungsmonitor erfolgt häufig über das Internet. Es ist zu gewährleisten, dass die Daten auf dem Übertragungsweg nicht von Unbefugten ausgelesen werden können. Hierfür ist eine Verschlüsselung einzusetzen.
- Die Videoüberwachung muss offen erfolgen. Sie ist durch erkennbare Hinweisschilder an dem überwachten Platz kenntlich zu machen.
- Die Aufzeichnungen dürfen höchstens einen Monat gespeichert werden. Es ist zu prüfen, ob auch eine kürzere Frist ausreichend ist.

Was ist zu tun?
Die Einrichtung einer Videoüberwachung ist wohl zu überlegen. Die Methode ist kein Allheilmittel gegen Gefahren und Straftaten. Will eine Kommune oder die Polizei diese für die Kontrolle öffentlicher Plätze nutzen, sind die datenschutzrechtlichen Anforderungen zu beachten.

4.2.10 Verfassungsbeschwerden gegen das Bundeskriminalamtgesetz

Im Jahr 2008 sind neue Regelungen im Bundeskriminalamtgesetz (BKAG) in Kraft getreten. Dem Bundeskriminalamt werden erstmals Aufgaben und Befugnisse zur Gefahrenabwehr zugewiesen. Das ULD hat gemeinsam mit den Datenschutzbeauftragten der Länder zu zwei dagegen gerichteten Beschwerden vor dem Bundesverfassungsgericht Stellung genommen.

Mit der Föderalismusreform I ist dem Bundeskriminalamt (BKA) im Grundgesetz die Zuständigkeit für die Abwehr von Gefahren des internationalen Terrorismus in bestimmten Fällen übertragen worden. Die neuen Vorschriften im BKAG regeln die Erfüllung dieser Aufgabe und verleihen dem BKA die hierfür **sehr weitreichenden Befugnisse**. Sie umfassen sämtliche im Polizeirecht bekannten verdeckten Ermittlungsmaßnahmen, u. a. verdeckte akustische und optische Wohnraumüberwachungen, Telekommunikationsüberwachungen, die Rasterfahndung und die sogenannte Online-Durchsuchung – teilweise unter Missachtung der verfassungsrechtlichen Anforderungen. Wir haben im verfassungsgerichtlichen Verfahren insbesondere folgende Kritikpunkte hervorgehoben:

- Der Schutz des Kernbereichs privater Lebensgestaltung ist nicht ausreichend gewährleistet. Für einige schwerwiegende Eingriffe sind keine Vorkehrungen zu dessen Schutz getroffen worden, so z. B. bei der akustischen Überwachung außerhalb von Wohnungen. Für die Online-Durchsuchung sowie die Telekommunikationsüberwachung sind die Schutzvorkehrungen unzureichend, da Überwachungsmaßnahmen nur dann unterbleiben müssen, wenn durch sie voraussichtlich *allein* Inhalte aus dem Kernbereich erlangt werden. Bei der Wohnraumüberwachung werden in Zweifelsfällen automatische Aufzeichnungen zugelassen, das sogenannte Richterband. Dies genügt unseres Erachtens nicht den verfassungsgerichtlichen Anforderungen zum Kernbereichsschutz bei Wohnraumüberwachungen.
- Das Gesetz räumt dem BKA umfangreiche Befugnisse im Vorfeld von Gefahren ein, ohne die Kriterien für ein Einschreiten in diesem Bereich mit der gebotenen Genauigkeit zu benennen.
- Das Gesetz bezieht in zu weitem Umfang sogenannte Kontakt- und Begleitpersonen ein, gegen die Maßnahmen ergriffen werden dürfen. Die Kriterien hierfür sind nicht immer ausreichend bestimmt.
- Für einige schwerwiegende Eingriffe fehlt der gebotene Richtervorbehalt, so z. B. für längerfristige Observationen oder akustische und optische Überwachungen außerhalb von Wohnungen.
- Die Benachrichtigungspflichten genügen nicht den verfassungsrechtlichen Anforderungen, soweit Benachrichtigungen zurückgestellt werden können, um den weiteren Einsatz eines verdeckten Ermittlers oder einer Vertrauensperson nicht zu gefährden. Gleiches gilt für die Möglichkeit, von einer Benachrichtigung ganz abzusehen, wenn die Voraussetzungen für eine Benachrichtigung in der Zukunft mit an Sicherheit grenzender Wahrscheinlichkeit nicht eintreten werden.

4.3 Justizverwaltung

4.3.1 Telefonieren im Strafvollzug – noch nicht die letzte Fortsetzung

Die Mängel beim Betrieb der Gefangenentelefonanlage im Strafvollzug konnten im Berichtszeitraum nicht abgestellt werden. Das ULD beanstandete den Betrieb der Anlage in einer Justizvollzugsanstalt und die Zusammenarbeit mit dem privaten Anbieter.



Die Mängel bei dem Einsatz der Gefangenentelefonanlage sind lange bekannt (32. TB, Tz. 4.3.5; 31. TB, Tz. 4.3.2). Für die Abwicklung und die Abrechnung der Gespräche, die Gefangene über die Telefonanlage führen, setzt die Justizvollzugsanstalt einen **externen Dienstleister** ein, der bundesweit solche Anlagen betreibt. Dort werden sämtliche personenbezogenen Daten über die Gefangenen, die für sie freigeschalteten Rufnummern sowie die Daten über geführte Telefonate ohne Rechtsgrundlage gespeichert. Die Datenverarbeitung durch den Dienstleister ist nur unzureichend vertraglich geregelt und dokumentiert. Die Justizvollzugsanstalt verfügt zudem faktisch über keine Kontrollmöglichkeiten, sodass die Datenverarbeitung durch den Dienstleister ingesamt nicht ausreichend transparent ist. Die Datenverarbeitung durch den externen Dienstleister sollte daher geändert und so ausgestaltet werden, dass dort keine personenbezogenen Daten über die Gefangenen und deren Gesprächspartner mehr verarbeitet werden. Dies ließ sich allerdings ohne Einbußen an dem bisherigen Serviceumfang nicht realisieren. Das ULD musste daher die erfolgende Datenverarbeitung beanstanden.

Was ist zu tun?
Unter Verzicht auf bestimmte angebotene Serviceleistungen ist die Verarbeitung auf pseudonymisierte Daten beim Dienstleister zu beschränken. Das Verfahren muss vollständig vertraglich geregelt und dokumentiert werden. Der Justizvollzugsanstalt müssen umfassende Kontrollmöglichkeiten eingeräumt werden.

4.3.2 Grundbucheinsicht für Versorgungsunternehmen

Einsicht in das Grundbuch können nur diejenigen nehmen, die ein berechtigtes Interesse darlegen, was grundsätzlich auch im automatisierten Abrufverfahren gilt. Ein Versorgungsunternehmen beantragte eine Ausnahme hiervon und wurde – zu Recht – vom zuständigen Grundbuchamt zurückgewiesen.

Die Grundbucheinsicht ist auch im automatisierten Verfahren grundsätzlich nur zulässig, wenn für das konkrete Grundstück ein berechtigtes Interesse dargelegt

wird. Hierfür ist beim Abruf ein bestimmter Grund anzugeben. Die Grundbuchverfügung macht von dieser Darlegungspflicht eine **Ausnahme: Versorgungsunternehmen**, z. B. Betreibern von Telekommunikationsanlagen, kann die Einsicht in allgemeiner Form für sämtliche Grundstücke eines Grundbuchbezirks gestattet werden, wenn sie ein berechtigtes Interesse hierfür darlegen. Die Entscheidung hierüber trifft das Grundbuchamt. Eine solche Ausnahme bedeutet für das Versorgungsunternehmen, dass es bei Abrufen im automatisierten Verfahren keinen Grund mehr angeben muss, aus dem sich das berechtigte Interesse ergibt.

Nachdem ein Grundbuchamt einen Antrag eines Versorgungsunternehmens abgelehnt hatte, bat dieses uns um eine Stellungnahme. Wir bestätigten dessen Rechtsauffassung. Die Ausnahmevorschrift in der Grundbuchverfügung erlaubt eine Ausnahmegenehmigung nur, wenn für jedes einzelne Grundstück im Grundbuchbezirk ein berechtigtes Interesse dargelegt wird. Besteht das **berechtigte Interesse für alle Grundstücke** nicht, kann die Ausnahmegenehmigung beschränkt erteilt werden, wenn eine sinnvolle Eingrenzung möglich ist. Wird das berechtigte Interesse nicht für alle Grundbucheinträge im Bezirk dargelegt und ist eine Beschränkung nicht möglich, kann die Genehmigung nicht erteilt werden. Die Unmöglichkeit einer Beschränkung kann nicht dazu führen, dass für sämtliche Grundstücke vollumfänglich ein berechtigtes Interesse angenommen wird.

Im vom Grundbuchamt zurückgewiesenen Antrag des Versorgungsunternehmens wurde das berechtigte Interesse damit begründet, dass das Unternehmen überprüfen müsse, ob und inwieweit tatsächlich Rechte an den von ihm genutzten Grundstücken bestehen. Außerdem müsse für künftig zu nutzende Grundstücke geklärt werden, wer Eigentümer des jeweiligen Grundstücks ist und welche Belastungen in der Abteilung II eingetragen sind. Den Bedarf für die Ausnahmegenehmigung hat das Unternehmen damit begründet, dass es nicht in jedem Einzelfall sicherstellen könne, dass die Berechtigung bezüglich des Grundstücks, dessen Grundbuchblatt es einsehe, tatsächlich entstanden oder vielleicht mittlerweile gelöscht worden ist. Zudem bedürfe es der Einsicht zu Grundstücken, die es erst noch für die Errichtung von Versorgungsinfrastruktur in Anspruch nehmen wolle. Offenbar ging das Unternehmen davon aus, dass es nicht an jeder von ihm beabsichtigten Einsicht ein berechtigtes Interesse haben würde. Ihm ging es also darum, eine **Befreiung von der Voraussetzung** des berechtigten Interesses als solchem und nicht nur von der Darlegung desselben zu erlangen. Dieses Ziel kann mit der Ausnahmegenehmigung nicht erreicht werden. Nach unserer Auffassung bestand übrigens in den genannten Fällen ein berechtigtes Interesse, sodass die Befürchtung des Antragstellers grundlos war.

Was ist zu tun?
Grundbuchämter sollten Anträge auf Gestattung der Einsicht in das Grundbuch in allgemeiner Form sorgfältig prüfen und ihnen nur so weit entsprechen, wie der Antragsteller ein berechtigtes Interesse an der Einsicht darlegt.

4.3.3 Vorabkontrolle einer neuen MESTA-Schnittstelle

Das bei den Staatsanwaltschaften eingesetzte Verfahren MESTA ist um eine Schnittstelle zum SAP-System des Landes erweitert worden.

Über die neue Schnittstelle sollen Rechnungsdaten aus dem Verfahren Mehrländer-Staatsanwaltschafts-Automation (MESTA) in das SAP-System übertragen werden. Dort werden sie vom **Finanzverwaltungsamt** weiterverarbeitet, das für die Justizbehörden in Schleswig-Holstein die Kassengeschäfte wahrnimmt. Da bei den Staatsanwaltschaften keine Datenschutzbeauftragten nach dem Landesdatenschutzgesetz bestellt sind, wurde das ULD mit der Durchführung der Vorabkontrolle beauftragt. In rechtlicher Hinsicht sprechen gegen die Einrichtung der Schnittstelle keine Bedenken. Wir haben aber empfohlen, weitere Maßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Insbesondere ist eine Protokollierung der über die Schnittstelle erfolgenden Übermittlungen einzurichten. Gleiches gilt für administrative Zugriffe, mit denen Änderungen am Programm bewirkt werden können. Der Generalstaatsanwalt zeigte sich diesen Anforderungen gegenüber aufgeschlossen und signalisierte Bereitschaft zu deren Umsetzung.

Was ist zu tun?
Bei allen automatisierten Verfahren gilt: Zugriffe von Administratoren sowie von Nutzern – zwecks Speicherung, Veränderung und Übermittlung der Daten – sind zu protokollieren. Auch die Protokollierung lesender Zugriffe der Nutzer entwickelt sich mehr und mehr zum Standard.

4.4 Verkehrsangelegenheiten: Fahrerlaubnisse außer Kontrolle?

Fast ein Jahr lang bewegte sich beim Datenschutz im Fahrerlaubniswesen in Sachen Datenschutz fast nichts, weil das zuständige Ministerium meinte, nicht zuständig zu sein. Nun besteht Hoffnung.

Im Januar 2010 wandte sich das ULD an das Ministerium für Wissenschaft, Wirtschaft und Verkehr mit einem umfangreichen Problemaufriss und einem Fragenkatalog zum Datenschutz im Fahrerlaubnisbereich. Hintergrund ist die Einführung des Zentralen Fahrerlaubnisregisters (ZFER) beim Kraftfahrt-Bundesamt (KBA) und die sukzessive Ablösung der dezentralen Papieraktenhaltung durch die bundesweite elektronische Datenverarbeitung, die erst im Jahr 2014 abgeschlossen sein wird, wenn die letzten Papier-„Lappen" der Vergangenheit angehören sollen. Wer berechtigt ein Kraftfahrzeug führt, hängt nicht nur vom Erwerb eines Führerscheins ab, sondern auch davon, ob dieser nicht wieder entzogen wurde, was beim KBA gesondert im Verkehrszentralregister gespeichert ist (VZR). Zwischen ZFER und VZR bestehen Querverweise. Da jedoch viele für die Fahrerlaubnis relevante Vorgänge noch aus der papierenen Zeit stammen, sind die **Fahrerlaubnisbehörden verunsichert**, welche Daten sie noch aufbewahren dürfen und welche – auch aus Datenschutzgründen – gelöscht werden müssen. Aus Kontrollen ist uns bekannt, dass hier im Land völlig unterschiedlich – oft weder praktikabel noch datenschutzkonform – verfahren wird. Das ULD hatte die Hoffnung, dass das Verkehrsministerium als Fachaufsicht den Behörden hier Hilfen gibt und klare Vorgaben macht.

Was dann folgte, war ein langer, unergiebiger Konflikt über die Frage, ob es zu den Aufgaben des Ministeriums gehört, solche Hilfen zu geben und Vorgaben im Bereich des Datenschutzes zu machen. Wir wiesen darauf hin, dass dies kein Eingriff in die **kommunale Selbstverwaltung** und in die Organisationshoheit der Kommunen ist und dass die Behörden ein großes Interesse an einer funktionierenden rechtskonformen Datenverarbeitung haben müssten, insbesondere wegen der Schnittstellen zum KBA und der Notwendigkeit der Beweissicherheit bei der Erteilung und dem Entzug von Führerscheinen. Es bedurfte schließlich der Information des zuständigen Landtagsausschusses, damit ein klärendes Gespräch zwischen ULD und Ministerium zustande kam. Es wurde verabredet, sich zeitnah zusammenzusetzen und gemeinsam eine Lösung zu suchen.

Was ist zu tun?
Das Verkehrsministerium sollte in enger Kooperation mit den Fahrerlaubnisbehörden und dem ULD Standards für einen datenschutzkonformen einheitlichen Umgang mit Fahrerlaubnisdaten erarbeiten.

4.5 Soziales

Die Sozialgesetzbücher sind eine dauernde Baustelle. Der darin vorgesehene Sozialdatenschutz wird bei Änderungen aber nur selten verbessert. Vielmehr scheint die Devise bei der Datenverarbeitung zu sein: **mehr, komplizierter, intransparenter, riskanter**. Gemäß diesem Motto wurde die Zuständigkeit für Datenschutzkontrollen beim Arbeitslosengeld auf den Bund übertragen (Tz. 4.5.1) und die Verfahren zur hausarztzentrierten Versorgung gestaltet (Tz. 4.5.3).

4.5.1 Ab 2011 ist das ULD nicht mehr für die ARGEn zuständig

Mit dem Gesetz zur Weiterentwicklung der Organisation der Grundsicherung für Arbeitssuchende wurde festgelegt, dass ab Januar 2011 für die Datenschutzkontrolle der ARGEn ausschließlich der Bundesbeauftragte zuständig ist.

Seit Einführung des Arbeitslosengeldes II (ALG II) im Jahr 2005 überwachten der Bundes- und die Landesbeauftragten für den Datenschutz **gemeinsam** die Einhaltung datenschutzrechtlicher Vorschriften bei den ARGEn bzw. Jobcentern. Zentrale Vorgaben der Bundesagentur für Arbeit (BA) prüfte der Bundesbeauftragte; die Landesbeauftragten waren für die Fragen der Betroffenen zum eigenen Fall zuständig. Damit ist nun Schluss. Diese Gesetzesänderung ist aus Datenschutzsicht ein gewaltiger Rückschritt. Es bestand keine Notwendigkeit, die in sechs Jahren erprobte und bewährte Zusammenarbeit zwischen dem Bundes- und den Landesbeauftragten „per Gesetz“ zu beenden und die Datenschutzaufsicht ins ferne Bonn zu verlagern.


https://www.datenschutzzentrum.de/presse/20100510-jobcenter.htm

Im Jahr 2010 waren Eingaben von ALG-II-Empfängern wieder ein Schwerpunkt unserer Arbeit. Viele Anliegen konnten unbürokratisch mit den Mitarbeitern in den ARGEn geklärt werden. Nun müssen die Betroffenen ihre Anliegen in Bonn vortragen. Auch wenn die Kollegen beim Bundesbeauftragten hervorragende Arbeit leisten, so sind sie doch von den Betroffenen wie den Ämtern räumlich weit entfernt. Die Bürger des Landes können sich künftig nicht mehr an ihren Landesbeauftragten wenden, um schnell und effektiv Hilfe zu bekommen. Wer in Schleswig-Holstein ALG II von einer ARGE bzw. einem Jobcenter erhält, muss und kann sich hierzu seit dem 1. Januar 2011 an den **Bundesbeauftragten für den Datenschutz und die Informationsfreiheit** in Bonn wenden.

Für die Kreise Schleswig-Flensburg und Nordfriesland, den **Optionskommunen**, in denen die Sozialzentren das Arbeitslosengeld II gewähren, bleibt das ULD jedoch weiterhin zuständig.

4.5.2 ELENA erfasste Millionen – bald wohl wieder gelöscht

Das ELENA-Verfahren hat in jeder Hinsicht Fortschritte gemacht. Die Rechtsgrundlagen wurden nachgebessert, der Katalog der zu übermittelnden Daten wurde reduziert. Im Praxisbetrieb sind inzwischen Millionen Datensätze gespeichert.

Es bleibt aber das grundsätzliche Problem: Stellt ELENA eine verbotene **Datenspeicherung auf Vorrat** dar? Die Bundesregierung beschloss im November 2010, dass ELENA – wenn überhaupt – erst im Jahr 2014 in den Wirkbetrieb gehen soll.

Im letzten Jahr hat sich einiges getan (32. TB, Tz. 4.5.15). Ende Februar 2010 ist die ELENA-Datensatzverordnung in Kraft getreten als formale **Rechtsgrundlage** für die Übermittlung einer Anzahl von Daten von den Arbeitgebern an die Zentrale Speicherstelle (ZSS). Die in der Verordnung verwendeten pauschalen Formulierungen sind immer noch nicht konkret genug und lassen zu viel Spielraum für Festlegungen durch die Verwaltung. So heißt es, „dass Daten zur Art der ausgeführten Tätigkeit sowie zu Beginn, Ende, Unterbrechung und Grund für die Beendigung des Beschäftigungsverhältnisses“ zu übermitteln sind. Präzisiert wird dies durch den sogenannten multifunktionalen Verdienstdatensatz (MVDS), der mittlerweile in der Version 0.2 von Juli 2010 vorliegt. Das Problem dieses Datenkatalogs ist, dass er durch Festlegungen eines demokratisch nicht legitimierten Gremiums zustande kommt. Positiv ist zu erwähnen, dass eine Reihe der ursprünglich vorgesehenen problematischen Datenfelder inzwischen aus dem Katalog entfernt wurde. Mittlerweile gibt es nur noch zwei Freitextfelder, die in einem speziellen Zusammenhang mit der Heimarbeit stehen und daher nur bei relativ wenigen Personen zur Anwendung kommen.

Verfassungsrechtliche Bedenken – vor allem im Hinblick auf eine unzulässige Vorratsdatenspeicherung – wurden in einer Sammelverfassungsbeschwerde von über 20.000 Personen gegen ELENA und das zugrunde liegende Gesetz geltend gemacht. Das Bundesverfassungsgericht hat in der Hauptsache noch nicht ent-

schieden. Im September 2010 wurde ein Eilantrag abgelehnt, weil die Eilbedürftigkeit nicht ausreichend dargelegt worden sei. Deshalb wurden zunächst weiter Daten an die ZSS gemeldet.

Bei **Aufnahme des Echtbetriebes** Anfang 2010 gab es Widerstände einiger Arbeitgeber und Arbeitnehmer gegen die erzwungenen Meldungen. Vielen Arbeitgebern war die Abgabe der Meldungen an die ZSS noch nicht möglich, weil die entsprechenden Schnittstellen und Routinen noch nicht in ihre Personalverwaltungssoftware implementiert waren. Mittlerweile haben alle namhaften Anbieter von Personalverwaltungssystemen eine ELENA-Schnittstelle eingebaut, sodass die Arbeitgeber, die diese Verfahren verwenden, die Daten ihrer Mitarbeiter in ELENA einmelden. Mitte Oktober 2010 lagen bei der ZSS bereits die Daten von über 30 Millionen Arbeitnehmerinnen und Arbeitnehmern mit insgesamt ca. 283 Millionen Datensätzen vor. Von ca. 180.000 möglichen Sendern, also Stellen, die Daten an die Zentrale Speicherstelle übermitteln können, sendeten zu diesem Zeitpunkt tatsächlich etwa 150.500 Sender Daten, was einer Quote von ca. 83 % entspricht. Die 150.500 Sender stehen dabei für ca. 2,5 Millionen Arbeitgeber, da sich viele, vor allem kleinere Arbeitgeber, anderer Stellen zum Senden der Daten bedienen.

Ursprünglich war als nächster Schritt angepeilt, die Daten für acht Sozialleistungsverfahren mit Beginn des Jahres 2012 zum Abruf bereitzustellen. Zuvor waren noch einige Probleme zu lösen, u. a. die Art und Weise der **Authentisierung der Sachbearbeiter** in den abrufberechtigten Stellen.

Ein wesentliches, noch ungelöstes Problem betrifft die Möglichkeit für die Betroffenen, eine **Selbstauskunft** über die bei der ZSS erfassten Daten zu erhalten. Die Auskunft soll grundsätzlich über die abrufberechtigten Stellen erfolgen. Da dafür noch keine Mechanismen zur Verfügung stehen, ist es gegenwärtig unmöglich, das Auskunftsrecht umzusetzen. Dies bedeutet, dass der Einzelne nicht prüfen kann, ob die in ELENA über ihn gespeicherten Daten korrekt sind. Wäre es ab 2012 zu einem Bezug von Sozialleistungen aufgrund der Daten in ELENA gekommen, so wäre nicht auszuschließen gewesen, dass falsche Daten gespeichert und Betroffenen deshalb nicht oder nicht sofort die Sozialleistungen zuteilgeworden wären, die ihnen zustehen.

Eine Möglichkeit, gleichwohl den Inhalt der Speicherungen bei der ZSS zu erfahren, besteht in einem **Auskunftsersuchen nach dem BDSG** beim Arbeitgeber, um zu erfahren, welche Daten von dort an ELENA gemeldet wurden. In Schleswig-Holstein vertreten einzelne große Arbeitgeber die Auffassung, das Auskunftsrecht aus den allgemeinen Datenschutzgesetzen sei dadurch ausgeschlossen, dass es spezielle Vorschriften zur Auskunft im Rahmen des ELENA-Verfahrens im Sozialgesetzbuch gibt. Diese Auffassung ist falsch. Die speziellen Auskunftsansprüche aus dem ELENA-Verfahren gelten neben den Auskunftsregelungen aus den allgemeinen Datenschutzgesetzen; keinesfalls schließen sie diese aus. Jede und jeder Beschäftigte hat das Recht, beim Arbeitgeber zu erfahren, welche Daten dieser an ELENA übermittelt hat.

Schon Mitte 2010 hatte der Bundeswirtschaftsminister vor allem aus Kostengründen gefordert, ELENA zu stoppen. Im November 2010 verständigte sich dann die Bundesregierung darauf, um zwei Jahre die **Testphase zu verlängern**. Erst 2014 soll der Datenabruf im Rahmen der Beantragung von Sozialleistungen beginnen. Da die schon erhobenen Daten so lange nicht auf Vorrat gespeichert werden dürfen, sind diese zumindest teilweise wieder zu löschen.

Was ist zu tun?
Die weitere Prüfung des Verfahrens sollte dazu führen, dass ELENA endgültig abgeschaltet wird. Wird an ELENA festgehalten, so muss dafür Sorge getragen werden, dass die Betroffenen zügig ihr Selbstauskunftsrecht wahrnehmen können.

4.5.3 Datenschutz bei der hausarztzentrierten Versorgung

Wegen drohender umfangreicher Datenschutzverstöße hat das ULD erstmalig eine Anordnung zur Regelung der Datenverarbeitung erlassen und diese für sofort vollziehbar erklärt. In dem betroffenen Bereich der hausarztzentrierten Versorgung muss eine Methode der Abrechnung gefunden werden, die den Datenschutzanforderungen entspricht.

Die Hausarztzentrierte Versorgung (HzV) ist eine besondere Versorgungsform im System der gesetzlichen Krankenversicherung. Der Hausarzt soll mehr als bisher eine Lotsenfunktion bei der Zuweisung des Patienten zu einzelnen Fachärzten wahrnehmen. Zudem werden dem Hausarzt konkrete Vorgaben im Hinblick auf die Qualitätssicherung seiner Arbeit, die leitlinienorientierte Behandlung und die Verschreibung bestimmter Medikamente gemacht. Ziel ist es, die Qualität der **Behandlung zu verbessern**. Gleichzeitig erhofft man sich eine Kostensenkung, z. B. weil nur bestimmte Medikamente, für die bei der jeweiligen Krankenkasse ein Rabattvertrag besteht, verschrieben werden. Für die Ärzte ist die Teilnahme an der HzV grundsätzlich freiwillig, doch erhalten sie einen erhöhten Vergütungssatz. Auch die Teilnahme der Patienten ist freiwillig. Diese sollen in erster Linie durch die u. a. finanziell motivierten Ärzte angeworben werden. Die Krankenkassen sehen die HzV überwiegend kritisch, weil sie Mehrausgaben fürchten, deren Effizienz umstritten ist.

Verträge zur HzV werden direkt zwischen den Krankenkassen und sogenannten Gemeinschaften von Leistungserbringern abgeschlossen; die üblicherweise tätige Kassenärztliche Vereinigung kommt hierbei nicht vor. Seit 2008 haben die Gemeinschaften der Leistungserbringer – dies sind zumeist die privatrechtlich organisierten **Hausärzteverbände** der einzelnen Bundesländer – das Recht, von den Krankenkassen den Abschluss eines entsprechenden Vertrages zu verlangen. Können sich die Gemeinschaften und die Kassen nicht auf den Inhalt des Vertrages einigen, so wird eine Schiedsperson eingesetzt, die den Vertrag festlegt.

In Schleswig-Holstein wurde **per Schiedsspruch** im September 2010 ein HzV-Vertrag zwischen dem Hausärzteverband Schleswig-Holstein sowie der Ärztegenossenschaft, die ebenfalls Hausärzte repräsentiert, einerseits und der AOK

Schleswig-Holstein (jetzt AOK NordWest, Tz. 4.5.4), der IKK Landesverband Nord sowie der Landwirtschaftlichen Krankenkasse Schleswig-Holstein und Hamburg andererseits abgeschlossen.

Neben Vorgaben zu den oben genannten Punkten enthält dieser Vertrag Regelungen zur Art und Weise der Datenverarbeitung im Rahmen der HzV. Betroffen sind hiervon im Datenschutzrecht besonders geschützte Daten über die Gesundheit, die zudem der ärztlichen Schweigepflicht unterliegen. Nach den Vorgaben des Gesetzes darf eine andere Stelle in die Abrechnung nur einbezogen werden, wenn dies im Wege einer **Auftragsdatenverarbeitung** nach den Vorgaben des Sozialgesetzbuches erfolgt. Das ULD informierte die Schiedsperson umfassend über die datenschutzrechtlichen Anforderungen. Dessen ungeachtet sah der Vertrag vor, dass die Datenverarbeitung zur Abrechnung bei der HzV über die Hausärztliche Vertragsgemeinschaft (HÄVG), eine eingetragene Genossenschaft in Köln, laufen soll. Diese soll, so die Fiktion des Vertrages, als Auftragnehmerin für die Hausärzte tätig werden.

Eine Analyse des Vertrages ergab, dass keine echte Datenverarbeitung im Auftrag vorliegt. Bei einer solchen bleiben nämlich die letzte Verantwortung und die Einflussmöglichkeiten auf die Verarbeitung bei den Auftraggebern, hier also bei den Hausärzten. Diese müssten die Möglichkeit haben zu bestimmen, in welcher Art und Weise ihre sensiblen Arztgeheimnisse verarbeitet werden. Dies ist aber im Vertrag nicht vorgesehen. Am augenfälligsten ist dabei eine technische Besonderheit: der Einsatz des sogenannten **gekapselten Kerns**. Dieser, nach der Herstellerfirma Inter Component Ware auch als ICW-Kern bezeichnet, ist ein Softwaremodul, welches die Hersteller der Praxisverwaltungssysteme in ihre Software einbauen müssen. Dabei kann der Arzt selbst nicht feststellen, welche Funktionen genau der gekapselte Kern wie erfüllt. Dieser hat keine eigene Oberfläche zur Interaktion mit dem Arzt. Die Hersteller der Praxisverwaltungssysteme sind vertraglich zum Stillschweigen darüber verpflichtet, wie die Schnittstelle zwischen Praxisverwaltungssystem und gekapseltem Kern genau ausgestaltet ist. Die Hersteller der Praxisverwaltungssysteme müssen sich sogar verpflichten, es zu unterlassen, den gekapselten Kern im Wege des Reverse Engineering zu untersuchen, um seine Funktionsweise zu ergründen. Aus Informatiksicht handelt es sich um eine Blackbox; lediglich die Personen, die das Softwaremodul programmiert haben, kennen seine genaue Funktionsweise. Die zur Abrechnung verwendeten Daten werden von den Praxisverwaltungssystemen an den gekapselten Kern weitergegeben und von dort verschlüsselt an die HÄVG gesendet. So können die einzelnen Ärzte nicht kontrollieren, welche Daten aus ihren Systemen abfließen. Es spricht einiges dafür, dass unter den derart abgezogenen Daten auch Informationen sind, die zu Abrechnungszwecken nicht weitergegeben werden dürften.

Das ULD sah sich deshalb veranlasst, gegenüber dem Hausärzteverband Schleswig-Holstein im Juli 2010 eine **Anordnung nach dem Bundesdatenschutzgesetz** zu erlassen. Dem Hausärzteverband wurde aufgegeben, dafür zu sorgen, dass keine von den Hausärzten im Zusammenhang mit der Durchführung des Vertrages erhobenen personenbezogenen Daten der Patienten an die HÄVG oder an andere in dem genannten Vertrag vorgesehene Unterauftragnehmer weitergegeben werden.


https://www.datenschutzzentrum.de/medizin/gkv/20100721-verfuegung-hzv.html

Das ULD erklärte die Anordnung für sofort vollziehbar. Für den Fall eines Verstoßes wurde ein Zwangsgeld in Höhe von 30.000 Euro angedroht. Gegen die Anordnung legte der Hausärzteverband Schleswig-Holstein Widerspruch ein und beantragte beim Verwaltungsgericht Schleswig die **Wiederherstellung der aufschiebenden Wirkung**. Der Widerspruch wurde vom ULD zurückgewiesen; hiergegen wurde Klage eingereicht. Nachdem das Verwaltungsgericht den Antrag des Hausärzteverbandes zurückgewiesen und dieser dagegen Beschwerde eingelegt hatte, entschied das Oberverwaltungsgericht Schleswig-Holstein (OVG) zugunsten des ULD und stellte fest, dass der HzV-Vertrag gegen materielles Datenschutzrecht verstößt. Es ging dabei in seiner Begründung noch über die Verfügung des ULD hinaus:

Es stellte fest, dass dem Arzt, der mit dem HzV-Vertrag verpflichtet wird, seine Patientendaten an die HÄVG weiterzugeben, keine Möglichkeit der Auswahl des Auftragnehmers gegeben wird. Will also ein Arzt an der HzV teilnehmen, bleiben ihm keine Alternativen. Er ist gezwungen, die sensiblen Daten an die HÄVG und deren Dienstleister weiterzugeben. Entgegen den Vorgaben des Gesetzes bestünden für den teilnehmenden Arzt keine oder zumindest nur geringe Einflussmöglichkeiten. Selbst eine Direktübermittlung der Abrechnungsdaten an die Krankenkasse wird ihm untersagt. Das OVG stellt klar, dass wegen der Verantwortlichkeit des Auftraggebers diesem die vollständige Einsichts- und **Kontrollmöglichkeit über die Datenverarbeitung** bewahrt bleiben muss, was den Hausärzten gegenüber der HÄVG im Vertrag jedoch verwehrt wird. Schließlich betont das OVG den Interessenwiderspruch, der im Fall eines Musterprozesses bei der Auftragsdatenverarbeitung nach Abtretung einer Ärzteforderung entstünde.

Das OVG prüfte zusätzlich zu den allgemeinen Voraussetzungen die der **sozialrechtlichen Auftragsdatenverarbeitung**. Es stellte fest, dass deren Voraussetzungen nicht vorliegen. Insbesondere die Unterbeauftragung durch die HÄVG steht im diametralen Widerspruch zum Gesetz, wonach der überwiegende Teil des Datenbestandes beim Auftraggeber verbleiben muss, was auch im Verhältnis Auftragnehmer zu Unterauftragnehmern gilt.


https://www.datenschutzzentrum.de/medizin/gkv/20110112-beschluss-ovg.pdf

Die gerichtliche Entscheidung ist von bundesweiter Bedeutung. Die Frage steht im Raum, ob die Hausärzteverbände und die HÄVG mit ihrer auch in anderen Bundesländern praktizierten Abrechnungsmethode fortfahren können. Nach dem Verdikt des OVG darf dies nicht sein. In Schleswig-Holstein wirkt sich das Urteil auf vier weitere HzV-Verträge aus. In den anderen Bundesländern teilen die Datenschutzaufsichtsbehörden die Rechtsauffassung des ULD und des OVG. Bei der hausarztzentrierten Versorgung müssen **datenschutzkonforme Abrechnungswege** gefunden werden. Das ULD hat hierzu Vorschläge gemacht und steht zur weiteren Beratung gern zur Verfügung.

Was ist zu tun?
Der Hausärzteverband Schleswig-Holstein, die Krankenkassen und die beteiligten Schiedspersonen müssen die Abrechnung zur hausarztzentrierten Versorgung endlich datenschutzkonform regeln und ausgestalten.

4.5.4 Aus der AOK Schleswig-Holstein wurde die AOK NordWest

Die AOK Schleswig-Holstein und die AOK Westfalen-Lippe fusionierten im Oktober 2010 zur AOK NordWest.

Die neue Krankenkasse hat ihren **Hauptsitz in Dortmund**. Zuständig für die Überwachung der Einhaltung datenschutzrechtlicher Vorschriften bei der AOK NordWest ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Zuständigkeit für eine gesetzliche Krankenkasse, die Versicherte von zwei Bundesländern betreut, hängt maßgeblich von ihrem Hauptsitz ab. Die Erreichbarkeitsdaten des Landesbeauftragten in Nordrhein-Westfalen finden sich im Internet.


https://www.datenschutz.de/institutionen/adressen/

Was ist zu tun?
Versicherte der AOK NordWest müssen nun ihre datenschutzrechtlichen Anliegen an den Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen richten.

4.5.5 TK-Ärztezentrum – Nicht überall, wo TK draufsteht, ist auch die TK drin!

Hinter einem TK-Ärztezentrum verbirgt sich ein externer Dienstleister. Die dort tätigen Ärzte unterliegen der ärztlichen Schweigepflicht. Personenbezogene Daten der Anrufer dürfen nicht ohne deren Einwilligung der TK übermittelt werden.

Ein Petent schilderte uns seine zunächst bestehende Begeisterung über das Angebot des TK-Ärztezentrums. An 365 Tagen erhalte man rund um die Uhr von qualifizierten Mitarbeitern **Auskunft zu medizinischen Fragen**. Dann kamen ihm Zweifel: Wird hier notiert, wer wie oft und warum anruft? Bei dem Gedanken, was passieren kann, wenn die falschen Stellen diese Informationen erhalten, wurde ihm mulmig.

In Absprache mit dem für die Techniker Krankenkasse (TK) zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) suchten wir das TK-Ärztezentrum im Gut Nehmten bei Plön auf. Fast 100 Ärztinnen und Ärzte sind dort damit beschäftigt, jährlich über 140.000 Anrufe entgegenzunehmen. Der Vorstand des Zentrums, der ife Gesundheits-AG, bestätigte uns, dass gespeichert wird, wer wann und aus welchem Grund anruft. Der TK werde u. a. eine „tägliche Kontakthistorie“ übermittelt. Diese enthalte neben der Versicher-

tennummer auch den Anrufgrund. Es bestand Konsens, dass diese Daten der ärztlichen Schweigepflicht unterliegen. Bei dem Dienstleister sah man jedoch keine Notwendigkeit, die Anrufer über die Übermittlung der Daten zu informieren bzw. diese um ihre Zustimmung zu bitten.

Gemeinsam mit unseren Kollegen vom BfDI mussten wir sowohl die TK sowie deren Dienstleister **eines Besseren belehren**. Jeder Anrufer muss zu Beginn des Telefonates ausdrücklich darauf hingewiesen werden, wer sich hinter dem TK-Ärztezentrum verbirgt, welche Daten gespeichert und welche Daten an die TK übermittelt werden. Die Anrufer müssen die Möglichkeit erhalten, einer Datenübermittlung zu widersprechen. Der BfDI forderte die TK auf, nach strengen Kriterien zu prüfen, welche Daten übermittelt werden müssen. Genügen nicht pseudonymisierte Daten? Die der TK übermittelten Daten unterliegen dort einer strengen Zweckbindung. Wir forderten von der ife Gesundheits-AG, dass ohne die Einwilligung der Anrufer nicht jeder Arzt der ife Gesundheits-AG auf die Dokumentationen früherer Anrufe zugreifen kann.

Was ist zu tun?
Sowohl die TK als auch die ife Gesundheits-AG müssen für eine ausreichende Transparenz für die Anrufer sorgen. Jeder Anrufer muss wissen, mit wem er telefoniert, welche Daten gespeichert werden, wer Zugang zu diesen Daten hat und welche Daten an die TK übermittelt werden. Für eine Datenübermittlung bedarf es der Einwilligung der Betroffenen.

4.5.6 Forschungsprojekt „Family Roots“

Das von dem Christlichen Jugenddorfwerk Deutschlands in Kreisen und kreisfreien Städten durchgeführte europäische Forschungsprojekt „Family Roots“ konnte durch die frühzeitige Datenschutzbegleitung datenschutzgerecht gestaltet werden.

Die Auswertung von **Akten der Jugendgerichtshilfen** und eine Befragung von Betroffenen sollte Aufschluss bringen, inwiefern die Familien von jugendlichen Straftätern in die Abläufe von Jugendstrafverfahren integriert werden. Doch dürfen die Mitarbeiter des Christlichen Jugenddorfwerk Deutschlands (CJD) zu diesem Zweck die Akten einsehen, sich Notizen machen bzw. Namen und Anschriften von Betroffenen an den CJD übermitteln? Für die Auswertung der Akten mussten die auf europäischer Ebene entwickelten Auswertungsbögen dem deutschen Datenschutzrecht angepasst werden. So wurden u. a. Datenfelder gestrichen, in denen nach dem Geburtsdatum gefragt wurde. Nur so war die beabsichtigte anonyme Datenerfassung zu gewährleisten. Weiter war zu klären, wer die Auswertung der Akten vornehmen sollte. In den Jugendgerichtshilfen fehlten die Zeit und das Personal. Das schleswig-holsteinische Landesdatenschutzgesetz erlaubt die Erfassung und Anonymisierung der Daten durch die Forschenden, wenn diese zuvor zur Verschwiegenheit verpflichtet wurden. Das CJD reichte umgehend Verpflichtungserklärungen ihrer Mitarbeiter nach.

Für die beabsichtigte **Interviewbefragung** wurde gemeinsam eine wirksame Schweigepflichtentbindungserklärung erarbeitet, die es den Jugendgerichtshilfen ermöglichte, bei Vorliegen der Unterschrift Namen und Kontaktdaten der Betroffenen an das CJD zu übermitteln.

Was ist zu tun?
Bei der Durchführung von Forschungsvorhaben sind datenschutzrechtliche Vorgaben zu beachten. Soll mit Daten öffentlicher Stellen geforscht werden, sind die forschenden Stellen gut beraten, schon im Vorfeld den Rat der behördlichen Datenschutzbeauftragten bzw. des ULD einzuholen.

4.5.7 Modellvorhaben „Fachberater für Menschen mit Behinderungen“

Gemeinsam mit dem Ministerium für Arbeit, Soziales und Gesundheit des Landes Schleswig-Holstein wurde sichergestellt, dass bei der Durchführung des Modellvorhabens „Fachberater für Menschen mit Behinderungen“ die Rechte der Betroffenen und die datenschutzrechtlichen Vorgaben beachtet werden.

Ziel des Modellvorhabens ist es, Unternehmen durch einen externen Fachberater bei der Suche nach Beschäftigungen für Menschen mit Behinderungen, bei **Besetzung und Sicherung solcher Arbeitsplätze** zu unterstützen. Zwangsläufig benötigt der Fachberater hierfür nicht nur Informationen über den jeweiligen Betrieb, sondern auch über die Betroffenen und deren gesundheitliche Einschränkungen. Zudem muss sich der Fachberater mit verschiedenen Betrieben und Behörden über diese Informationen austauschen.

Sowohl das Erheben als auch das Übermitteln von Daten ist nur mit der ausdrücklichen Einwilligung der Betriebe und der Menschen mit Behinderungen zulässig. Für eine wirksame Einwilligung ist die Transparenz der beabsichtigten Datenerhebung und -übermittlung entscheidend. Gemeinsam mit dem Ministerium wurden detaillierte Informationstexte und datenschutzgerechte Einwilligungserklärungen erarbeitet. Hierbei wurde auf die im Jahr 2009 mit dem damals zuständigen Ministerium entwickelten Mustererklärungen und Hinweistexte für einen Datenaustausch zwischen Jugendgerichtshilfen und Arbeitsämtern bzw. Jobcentern zurückgegriffen (32. TB, Tz. 4.5.13).

Was ist zu tun?
Damit ein „Fachberater“ Daten von Betrieben und Menschen mit Behinderungen erheben, speichern und mit anderen Stellen oder Behörden austauschen darf, bedarf es der wirksamen Einwilligung der Betroffenen.

4.5.8 Vorbildliche Schulungen: die Mürwiker Werkstätten

Eine qualifizierte engagierte betriebliche Datenschutzbeauftragte kann vieles bewegen. Ihre Arbeit hängt aber von ihren Kolleginnen und Kollegen ab. Will ein Unternehmen einen hohen Datenschutzstandard erreichen, muss die gesamte Belegschaft mit dem Datenschutz vertraut sein.

Die Bemühungen der Mürwiker Werkstätten sind insofern vorbildlich. Seit 2006 ermöglicht die Geschäftsführung nahezu allen (!) Mitarbeiterinnen und Mitarbeitern, an **Schulungen der DATENSCHUTZAKADEMIE Schleswig-Holstein** teilzunehmen. Der Erfolg kann sich sehen lassen. Werkstatt- und Heimverträge wurden datenschutzgerecht gestaltet, Schweigepflichtentbindungserklärungen erarbeitet und das Verständnis der Kollegen dafür, wer welche Daten der Klienten benötigt und welche Anfragen von welchen Stellen beantwortet werden dürfen, erhöht. Besonders hervorzuheben ist die durchgeführte Schulung von den zu betreuenden Beschäftigten, die in einzelnen Werkstatt- oder Arbeitsbereichen in Berührung mit personenbezogenen Daten kommen können.

Was ist zu tun?
Um ein hohes Datenschutzniveau zu erreichen, ist es erforderlich, jeden Mitarbeiter der Behörde bzw. des Wirtschaftsunternehmens mit den Vorschriften zum Datenschutz vertraut zu machen. Ein Schulungskonzept ist hierfür Gold wert.

4.6 Schutz des Patientengeheimnisses

4.6.1 Die neue Orientierungshilfe für Krankenhausinformationssysteme − KIS

Die neue „Orientierungshilfe KIS“ formuliert aus den datenschutzrechtlichen Regelungen und den Vorgaben zur ärztlichen Schweigepflicht konkrete Forderungen für den Krankenhausbetrieb und die Anwendung von Informationssystemen in Krankenhäusern.



Adressaten dieser Orientierungshilfe sind neben den Krankenhäusern die Systemhersteller von Verarbeitungsprogrammen. Viele Krankenhäuser haben die Tendenz zu „schwarzen Löchern“: Unmengen sensibelster Patientendaten verschwinden in der als Krankenhausinformationssystem – KIS − bezeichneten EDV. Die „Orientierungshilfe KIS“ wurde unter der Federführung des Berliner Beauftragten für Datenschutz und Informationsfreiheit durch eine Unterarbeitsgruppe der **Arbeitskreise „Gesundheit und Soziales“ und „Technik“** der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet. Ausgangspunkt war ein vom Hamburgischen Datenschutzbeauftragten erstelltes Eckpunktepapier. Eine Einbindung der Hersteller von KIS, z. B. von

Siemens Healthcare, Nexus und AGFA, erfolgte ebenso wie eine Expertenbefragung u. a. in Krankenhäusern und bei Verbänden. Die Verarbeitung der Patientendaten wird sowohl für die medizinische Behandlung, für die Pflege und für die Verwaltung vorgenommen. Durch die Orientierungshilfe soll sichergestellt werden, dass Mitarbeiter eines Krankenhauses nur auf die Daten Zugriff haben, die sie für ihre Aufgabe benötigen. Es gilt das Prinzip des „**Need-to-know**“. Es darf nicht sein, dass z. B. im Universitätsklinikum Schleswig-Holstein 5.500 Mitarbeiter einen unbeschränkten Zugriff auf sämtliche Patientendaten hatten (Tz. 4.6.2).



Im Teil I der Orientierungshilfe, den „Normativen Eckpunkten zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus“, werden klare Aussagen getroffen, welche Mitarbeiter eines Krankenhauses wann Zugriff auf welche Daten eines Patienten haben dürfen. Die Datenverarbeitung in der Aufnahme, während der Behandlung, in der Abrechnung oder im Archiv wird detailliert dargestellt. Es finden sich Aussagen zu Konsiliar- und Chefärzten, zu Administrationskräften und zum Medizincontrolling. Im Teil II, den „Technischen Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“, werden Maßnahmen zur technischen Umsetzung dieser Anforderungen beschrieben. Durch Beschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder soll sichergestellt werden, dass diese „Orientierungshilfe KIS“ **bundesweit zu beachten** ist.

Was ist zu tun?
Betreiber von Krankenhäusern und die Hersteller von Krankenhausinformationssystemen müssen die in der „Orientierungshilfe KIS“ aufgestellten datenschutzrechtlichen Anforderungen beachten.

4.6.2 Zugriffsrechte im KIS des Universitätsklinikums Schleswig-Holstein

Daten über die Gesundheit von Patienten sind besonders zu schützen. Dazu gehört es auch, den Zugriff auf Informationen über frühere Behandlungen in Krankenhäusern auf solche Personen zu beschränken, die diese Informationen tatsächlich benötigen.

Die Verarbeitung personenbezogener Daten zum Zweck der Dokumentation, der Behandlung, der Abrechnung und der Archivierung erfolgt in Krankenhäusern in der Regel mithilfe sogenannter Krankenhausinformationssysteme (KIS). Beim Universitätsklinikum Schleswig-Holstein (UK S-H) wird dazu das System ORBIS verwendet. Bei der Administration solcher Systeme ist darauf zu achten, dass **Zugriffsrechte** tatsächlich nur im jeweils erforderlichen Umfang gewährt werden. Grundsätzlich ist der Zugriff auf die bei einer medizinischen Organisationseinheit, z. B. einer Station, beschäftigten Mitarbeiter zu beschränken.

Das ULD hatte Hinweise erhalten, dass im System ORBIS beim UK S-H die Zugriffsrechte zu weitgehend sind. Zwar waren Details der Krankengeschichte nur für die jeweils behandelnde Organisationseinheit zugänglich. Jedoch konnten sämtliche Mitarbeiter mit Zugangsberechtigung zum System ORBIS feststellen, in welchen anderen Organisationseinheiten ein Patient bereits in der Vergangenheit behandelt wurde. Aus diesen Informationen lassen sich bereits sehr konkrete Rückschlüsse über die Art der Erkrankung ziehen. Dies kann z. B. im Hinblick auf psychologische oder psychiatrische Behandlungen für den Betroffenen stigmatisierende Folgen haben. Probleme bestehen zudem für die zahlreichen Mitarbeiterinnen und Mitarbeiter des UK S-H, die sich beim Arbeitgeber behandeln lassen. Sie mussten damit rechnen, dass ihre Kollegen einfach die Tatsache der Behandlung in bestimmten Einrichtungen feststellen konnten. Unsere Überprüfung ergab, dass insgesamt ca. 5.500 Mitarbeiter, also etwa **die Hälfte des Personals des UK S-H, unbeschränkten Zugriff** auf diese Informationen hatte. Es genügte, einen beliebigen Namen einzugeben. War die Person behandelt worden, so konnte der Abfrager erkennen, in welchen Einrichtungen dies erfolgt war.

Diese Situation ist aus Datenschutzsicht nicht hinnehmbar (Tz. 4.6.1). Beim UK S-H wurden **organisatorische und technische Umstellungen** vorgenommen. Eine Nachschau des ULD im September 2010 ergab, dass jetzt nur noch ca. 300 Verwaltungsmitarbeiter den oben beschriebenen Zugriff haben. Dabei handelt es sich um Personen, die die Patienten aufnehmen, um Mitarbeiterinnen und Mitarbeiter des Patientenmanagements und des Medizincontrollings. Damit ist davon auszugehen, dass nur noch die tatsächlich zuständigen Personen den beschriebenen Zugriff haben. Wird eine Person in einer Einrichtung aufgenommen, so haben die jeweiligen Mitarbeiter dieser medizinischen Einrichtung den Zugriff auf die Vorbehandlungen und zudem auf die sogenannte zentrale Krankengeschichte, die Details über die aktuelle und gegebenenfalls auch frühere Behandlungen enthält.

Mit dem UK S-H besteht Einigkeit, dass es für Patientinnen und Patienten die Möglichkeit geben soll, eine Pseudonymisierung ihrer Daten in der Weise zu erhalten, dass bestimmte Vorbehandlungen komplett ausgeblendet werden. Dies kann allerdings erst bei der Archivierung, d. h. nach der Abrechnung der jeweiligen Behandlung, erfolgen. Dazu ist es erforderlich, dass sich diejenigen, die dies wünschen, an den Datenschutzbeauftragten des UK S-H mit folgenden Kontaktdaten wenden:



http://www.uk-sh.de/Patienten+_+Besucher/Fix_
Navigation+/Organisation/Verwaltung/Datenschutz-p-19148.html

Was ist zu tun?
Das UK S-H muss, wie alle Krankenhäuser in Schleswig-Holstein, anhand der in Tz. 4.6.1 beschriebenen Anforderungsliste konkrete Anforderungen an die Hersteller von Krankenhausinformationssystemen stellen, damit diese die zur Wahrung des Datenschutzes erforderlichen Eigenschaften in die Programme einbauen, und dann die entsprechenden Einstellungen bei der Implementierung vornehmen.

4.6.3 Keine Infos über HIV und Hepatitis für den Rettungsdienst

Informationen über bestehende Infektionskrankheiten sind hochsensibel. Wünsche, an solche Informationen zu kommen, sind nicht immer stichhaltig begründet.

Darf ein Krankenhaus dem Personal eines Rettungsdienstes bei der Übergabe eines Patienten Informationen zu bestehenden Infektionskrankheiten mitteilen? Die Rettungsdienstleitung eines Kreises forderte die standardmäßige Mitteilung von Infektionskrankheiten wie HIV oder Hepatitis B und C. Die Übertragung erfolgt ausschließlich durch **Kontakt von Körperflüssigkeiten** und ist durch die im Rettungsdienst üblichen Schutzmaßnahmen wie das Tragen von Handschuhen vermeidbar. Ein Restrisiko für die Rettungsdienstmitarbeiter ist nicht zu leugnen, muss aber gegenüber dem Interesse des Patienten an der vertraulichen Behandlung der besonders sensiblen Informationen abgewogen werden.

Bei hochansteckenden und gefährlichen Infektionskrankheiten wie Tuberkulose, Influenza oder SARS sind **besondere Hygienemaßnahmen** im Rettungsdienst erforderlich. Dementsprechend muss auch die Rettungsdienstbesatzung darüber informiert werden, damit die Hygiene- und Selbstschutzmaßnahmen erfolgreich getroffen werden können. Dann darf auch die konkrete Erkrankung benannt werden. Bei über Kontakt übertragenen Infektionskrankheiten, die durch empfohlene Hygienemaßnahmen vermeidbar sind, kann mitgeteilt werden, dass eine Infektionskrankheit vorliegt, ohne diese genau zu benennen. Ansonsten genügen die Standardhygienemaßnahmen; eine Mitteilung an den Rettungsdienst ist nicht statthaft. Dies gilt für Erkrankungen, die ausschließlich über Blutkontakt oder Stichverletzungen übertragen werden können, wie z. B. Hepatitis und HIV.

Gerade bei HIV und Hepatitis muss das Interesse des Patienten auf informationelle Selbstbestimmung besonders beachtet werden. Auch der Gesetzgeber hat erkannt, dass eine HIV-Erkrankung zu einer **besonderen Stigmatisierung** des Betroffenen führen kann, und hat auf eine namentliche Meldepflicht im Informationsschutzgesetz verzichtet. Das Interesse des Patienten überwiegt gegenüber dem bestehenden Restrisiko einer Infektion. Wichtig ist die Beachtung der vorgeschriebenen Schutzmaßnahmen durch das medizinische Personal.

Was ist zu tun?
Das den Patienten entlassende ärztliche Personal muss entscheiden, ob und inwieweit der Rettungsdienst über eine Infektionskrankheit informiert wird. Der konkrete Erreger ist nur bei hochinfektiösen und gefährlichen Infektionskrankheiten zu benennen.

4.6.4 Die wundersame Datenmehrung bei der Trennung von Gemeinschaftspraxen

Streit kann auch bei Ärzten entstehen, die sich zur Berufsausübung zusammentun. Die Trennung von Gemeinschaftspraxen wirft oft datenschutzrechtliche Probleme auf.

Patienten einer von mehreren Ärzten betriebenen Gemeinschaftspraxis haben den Vorteil, in Urlaubszeiten einen leidlich bekannten medizinischen Ansprechpartner zu haben. Der Behandlungsvertrag gilt rechtlich zwischen dem Patienten und sämtlichen in der Gemeinschaftspraxis tätigen Ärzten. Trennt sich so eine Gemeinschaftspraxis, fühlen sich nicht selten alle Ärzte berufen, sämtliche Patientenakten fortan zu verwahren. Bei Papierakten war dies selten ein Problem, weil diese schon aus Praktikabilitätsgründen aufgeteilt wurden. Dies hat sich mit der **digitalen Aktenhaltung** geändert. Schnell ist der gesamte Datenbestand der Praxissoftware kopiert.

Diese wundersame Datenmehrung ist aus Datenschutzsicht höchst unwillkommen. Das Risiko, dass Daten in unbefugte Hände gelangen, wird vervielfacht. Richtigerweise sind auch im Digitalzeitalter die Patientenakten danach zu trennen, welcher der Ärzte fortan die Behandlung führt. Steht dies noch nicht fest, verbleiben die Akten bei der Praxis, die **in den alten Räumen** bleibt. Um festzustellen, ob ein Patient bereits in der früheren Gemeinschaftspraxis in Behandlung war, dürfen alle scheidenden Praxispartner für eine Übergangszeit von der Gesamtheit der Patienten die Stammdaten nebst Aktenzeichen vorhalten.

Ärzte kritisieren, dies sei zu aufwendig. Einfacher und praktikabel wäre es, bereits beim Betrieb der Gemeinschaftspraxis die **Daten sauber zu trennen**, wie dies Praxisgemeinschaften – das sind Praxen, in denen Ärzte sich lediglich die Räume teilen – ohnehin tun müssen. Für die Dauer der gemeinsamen Praxisausübung können gegenseitige Zugriffsrechte eingeräumt werden, die dann bei der Teilung aufgehoben würden.

Was ist zu tun?
Bei der Trennung von Gemeinschaftspraxen ist eine Datenduplizierung zu vermeiden und frühestmöglich durch eine Löschung oder Sperrung der Daten aufzuheben. Idealerweise werden Akten schon mit Aufnahme der Tätigkeit nach Ärzten getrennt geführt.

4.6.5 Gesichtsfoto von Patienten für Patientenakte bedarf der Einwilligung

Eine Arztpraxis fotografierte ohne wirksame Einwilligung der Patienten das Gesicht für die Patientenakte. Verheimlichungsversuche des Arztes gaben Anstoß zu Spekulationen über die Verwendung der Fotos.

Ein Patient erspähte sein Gesichtsbild auf dem Bildschirm des Systems der Facharztpraxis für Urologie und Geschlechtskrankheiten. Die Verheimlichungsstrategie des Arztes schürte offensichtlich das Misstrauen der Betroffenen und Speku-

lationen über die Verwendung. Wurden gar heimliche Fotos bei der Behandlung gemacht? Die Betroffenen wurden nur teilweise auf die Anfertigung der Fotos hingewiesen. Eine **richtige Aufklärung** fehlte.

Der Arzt rechtfertigte die Bilder damit, er könne sich beispielsweise bei telefonischen Rückfragen besser an die einzelnen Fälle erinnern. Dies ist nachvollziehbar, liegt es doch auch im **Interesse der Patienten**, dem Gedächtnis des Arztes auf die Sprünge zu helfen. Die Einbindung von Fotos in die Behandlungsakte kann zudem den Umgang mit den Daten der Patienten verbessern, die im Wartezimmer direkt und ohne Nennung des Namens angesprochen werden können.

Bildaufnahmen sind personenbezogene Daten, deren Verarbeitung einer Rechtsgrundlage bedarf. Für eine ärztliche Behandlung sind Fotos außerhalb der Behandlungsdokumentation nicht erforderlich. Mangels gesetzlicher oder vertraglicher Grundlage bedarf es für ein Fotografieren der Patienten und Speichern der Bilder der **Einwilligung der Patienten**, die eine Unterrichtung über die Verwendungszwecke voraussetzt. Angesichts der nachvollziehbaren Gründe für die Fotoaufnahme werden Patienten eine Einwilligung in der Regel nicht verweigern. Umso unverständlicher war die unterlassene Unterrichtung der Patienten vor der Aufnahme und über deren Zweck. Ohne Einwilligung angefertigte Bildaufnahmen sind zu löschen. Bei den zur Wiedererkennung angefertigten Bildern handelte es sich nicht um handlungsrelevante Daten, die als Teil der Patientenakte zu verwahren waren. Die Praxissoftware muss die Löschung der Bilder technisch vorsehen.

Was ist zu tun?
Wer von Kunden oder Patienten zusätzliche Daten wie ein Gesichtsbild erheben will, benötigt eine Einwilligung der Betroffenen. Diese sind zuvor über die Art der Daten und deren Verwendungszweck zu unterrichten.

4.6.6 Wenn einem Arzt der Laptop gestohlen wird

Ärzte sind gut beraten, wenn sie ihre elektronischen Patientendaten verschlüsselt speichern. Nur so ist auszuschließen, dass bei Verlust eines Rechners oder eines Laptops der „Finder“ Kenntnis von Patientendaten erhält.

Wir staunten nicht schlecht, als uns ein **gebrauchter Laptop** übergeben wurde, der auf diversen Umwegen in den Besitz des Überbringers geraten war. Darauf befanden sich neben „Schmuddelgeschichten“ auch unverschlüsselte Patientendaten einer Arztpraxis. Auf dem Gerät war spezielle Software für Arztpraxen installiert. Problemlos konnten 342 Word-Dokumente mit Patientendaten geöffnet werden. Es handelte sich überwiegend um ärztliche Bescheinigungen und Arztbriefe einer Kinderarztpraxis.

Die Kinderarztpraxis erklärte uns, dass nicht nur dieser Laptop, sondern weitere drei Laptops und zwei Rechner bei einem Einbruch gestohlen wurden. Die Polizei bestätigte, dass die Einbrecher mit erheblicher Gewalt vorgegangen waren. Wir konnten der Kinderarztpraxis zwar keinen Verstoß gegen datenschutzrechtliche

Bestimmungen vorwerfen, da, so die Polizei, „ausreichende Schutzmaßnahmen gegen Einbruch“ getroffen worden waren. Dennoch haben wir die Praxis aufgefordert, Patientendaten künftig verschlüsselt zu speichern. Schlimm genug, wenn bei einem Einbruch der Laptop gestohlen wird. Die Folgen für die Patienten, wenn deren Daten in unbefugte Hände gelangen, können jedoch noch wesentlich fataler sein. Das ULD gibt gern Hinweise und Hilfen zur **Verschlüsselung von Daten**. Ärzte sollten die Anbieter ihrer Arztpraxissoftware auf Verschlüsselungsmöglichkeiten ansprechen.

Was ist zu tun?
Daten von Patienten, die der ärztlichen Schweigepflicht unterliegen, sollten grundsätzlich nur verschlüsselt gespeichert werden.

4.6.7 Missglückte Befundversendung beim Mammografie-Screening

Datensicherheitspannen haben ärgerliche Folgen für die Betroffenen. Das Instrument der sogenannten Security Breach Notification soll diese Folgen mildern. Es hat sich bereits kurz nach seiner Einführung ins Bundesdatenschutzgesetz bewährt.

Das ULD befasst sich seit Jahren mit dem Datenschutz beim Mammografie-Screening (32. TB, Tz. 4.5.11). Jetzt ereilte uns die Meldung über einen Datenschutzverstoß bei dem Versenden von Befundmitteilungen. Es war in einer der Screening-Einheiten in Schleswig-Holstein zu einer **Fehlprogrammierung einer Kuvertiermaschine** gekommen. Dadurch wurden versehentlich bei ca. 75 der von der Screening-Einheit zur Befundmitteilung an die Teilnehmerinnen versandten Fensterbriefumschläge nicht nur, wie eigentlich vorgesehen, ein Blatt, sondern zwei Blätter eingelegt. Die Kuvertiermaschine verfügte über zwei einprogrammierte Routinen. Die eine zur Versendung lediglich eines Blattes in einem Fensterbriefumschlag sollte für Befundversendungen an die Teilnehmerinnen verwendet werden. Die zweite für die Kuvertierung von zwei Blättern sollte für bestimmte Mitteilungen an Ärzte Verwendung finden. Versehentlich wurde zur Versendung der Befundmitteilungen die für Ärzte vorgesehene Routine eingeschaltet. Dadurch erhielt die Hälfte der Frauen, deren Befundmitteilung an einem bestimmten Tag verschickt wurde, nicht nur ihren eigenen Befund, sondern auf einem zweiten Blatt den Befund einer anderen Frau. Die andere Hälfte der betroffenen Frauen bekam gar keine Mitteilung. Im Nachhinein ließ sich nicht mehr klären, welche Frauen jeweils betroffen waren.

Eine Neuregelung des Bundesdatenschutzgesetzes verpflichtet verantwortliche Stellen, die Datenschutzaufsichtsbehörde sowie die betroffenen Personen über einen solchen Verstoß zu informieren, wenn es hierbei zur **unrechtmäßigen Kenntniserlangung** von Daten durch Dritte gekommen ist und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Wie vorgesehen informierte die Screening-Einheit das ULD und auch die betroffenen Frauen über den Zwischenfall.

Als Reaktion wurde zur Vermeidung künftiger gleichartiger Vorfälle die Programmierung so geändert, dass nur noch die Routine zur Versendung von einem Blatt zur Verfügung steht. Da die Daten verarbeitende Stelle, wie gesetzlich vorgesehen, eine Meldung über den Vorfall an das ULD abgab, kam eine weitere Sanktionierung, z. B. durch ein Bußgeld, nicht mehr in Betracht. Insoweit profitieren die verantwortlichen Stellen von der sogenannten **Security Breach Notification**, wenn sie diese ordnungsgemäß abgeben.

Was ist zu tun?
Mögliche Schwachstellen bei der Einhaltung der Datensicherheit sollten im Vorfeld erkannt und beseitigt werden. Kommt es gleichwohl zu Zwischenfällen, bei denen Dritte unrechtmäßig Kenntnis von Daten erlangen, so sind darüber das ULD als Aufsichtsbehörde sowie die Betroffenen zu informieren.

4.6.8 Wenn ein Augenoptiker seine Kundendaten verkaufen will

Ein Augenoptiker unterliegt nicht der ärztlichen Schweigepflicht, darf aber Daten seiner Kunden nicht ohne deren Einwilligung veräußern. Bei einer Geschäftsübergabe ist auch das „2-Schrank-Modell" zu praktizieren.

Kundendaten eines Augenoptikers sind in großem Umfang auch **Angaben zur Gesundheit**. Der Verkauf dieser Daten stellt eine Übermittlung dar, für die es einer ausreichenden Befugnis bedarf. Mangels gesetzlicher Übermittlungsbefugnis kommt ausschließlich die wirksame Einwilligung der betroffenen Kunden in Betracht.

Ein Optiker hatte die Kundendaten eines Petenten verkauft, ohne diesen zu fragen. Der Optiker begründete dies damit, dass der Erwerber seines Geschäftes u. a. Garantie- und Gewährleistungsansprüche abdecken würde. Zudem sei es für eine „vollständige Versorgung hilfreich, die augenoptische Vorgeschichte eines Kunden zu kennen". So gut gemeint dies sein mag, so ersetzt das nicht die Einwilligung der Kunden. Sicher ist es nicht möglich, jeden Kunden zu befragen, ob dieser mit der Veräußerung seiner Daten einverstanden ist. Dies berücksichtigt das von den Ärztekammern entwickelte und von den Datenschutzaufsichtsbehörden akzeptierte „**2-Schrank-Modell**". Dabei übernimmt der Erwerber Kundendaten zwar ohne deren Einwilligung, verwahrt diese jedoch getrennt von seinem eigenen Datenbestand – in einem zweiten Schrank. Wenn ein Kunde tatsächlich bei ihm vorspricht, können dessen Daten genutzt werden. Die Daten jener Kunden, die in einer zu bestimmenden Frist nicht beim Erwerber vorsprechen, werden gelöscht, ohne dass sie der Erwerber zur Kenntnis nimmt. Wir haben den Optiker, der die Daten erworben hat, aufgefordert entsprechend zu verfahren, und darauf hingewiesen, dass eine Nutzung der gesperrten Daten ohne die Einwilligung der Betroffenen eine Ordnungswidrigkeit darstellt.

Was ist zu tun?
Die Veräußerung von Kundendaten eines Augenoptikers bedarf der Einwilligung der Betroffenen. Fehlt diese, so ist bei der Übergabe der Kundendaten das „2-Schrank-Modell“ zu praktizieren. Eine Verarbeitung dieser Daten des Altkundenschranks ist erst möglich, wenn der Kunde beim Erwerber vorspricht und hierdurch seine Einwilligung erklärt.

4.6.9 AOK-Arztnavigator – Teufelswerk oder vorbildliches Bewertungsportal?

Internetportale zur Bewertung beruflicher Leistungen bergen erhebliche Risiken für den Datenschutz. Sie sind aber nicht grundsätzlich verboten. Es kommt darauf an, solche Portale datenschutzkonform auszugestalten.

Zur Bewertung von niedergelassenen Ärzten gibt es eine Reihe von Bewertungsportalen im Internet. Alle zeichnen sich, wie eine Studie nachgewiesen hat, durch Mängel aus. Im Zusammenhang mit der Initiative der Bertelsmann Stiftung, für **mehr Transparenz im Gesundheitswesen** zu sorgen, der sogenannten Weissen Liste, hat die Stiftung zusammen mit der AOK ein Arztbewertungsportal aufgebaut, das die Fehler der anderen vermeiden soll. Das ULD wurde gegen Entgelt zu einzelnen datenschutzrechtlichen Fragen um Beratung gebeten. Damit sollte nicht der rechtlichen Beurteilung durch die örtlich zuständigen Datenschutzaufsichtsbehörden vorgegriffen werden. Den Portalbetreibern ging es darum, bereits im Vorwege möglichst datenschutzkonforme Lösungen zu finden.

Nach Meinung des ULD ist dies gelungen. Das Konzept zielte von Anfang an darauf ab, die Rechte der bewerteten Ärzte so wenig wie möglich zu beeinträchtigen. Den Patientinnen und Patienten, die die Ärzte bewerten wollen, wird ermöglicht, ihre Bewertungen ohne Aufdeckung ihres Personenbezugs, also praktisch anonym, abzugeben. Rechtliche Leitschnur zur Gestaltung von Bewertungsportalen ist das Urteil des Bundesgerichtshofes (BGH) zum **Lehrerbewertungsportal „Spick mich“**. Der BGH stellte fest, dass „Spick mich“ in der vom Gericht untersuchten Ausgestaltung zulässig war und keine Verletzung des Datenschutzrechts darstellte.

Einige Eigenschaften des Lehrerbewertungsportals ließen sich auf Arztbewertungsportale aber nicht übertragen. So war der Zugriff auf die Bewertungen im Grundsatz nur für die Schulöffentlichkeit möglich. Im Hinblick auf die freie Arztwahl in Deutschland kann es eine entsprechende Beschränkung bei Ärzten nicht geben. Beim Arztnavigator wurde jedoch für einen im Ergebnis gleichartigen Schutz der Persönlichkeitsrechte der Ärzte gesorgt. Ein Log-in zur Bewertung wird nur an Versicherte der AOK vergeben; eine Erweiterung auf andere Krankenkassen in der Zukunft ist vorgesehen. Auf pseudonymer Basis wird geprüft, ob eine Person, die Bewertungen zu Ärzten abgeben will, tatsächlich bei der AOK versichert ist. Nur dann kann sie eine Bewertung für einen Arzt abgeben. So wird verhindert, dass Bewertungen durch Patienten oder die Ärzte selbst verfälscht werden, z. B. indem von einer Person zu einem Arzt mehrere Bewertungen abgegeben werden. Weitere **Schutzmechanismen** sind der Verzicht auf Freitextfelder, ein strukturierter Fragebogen, der Extremaussagen ausschließt, und die Vorgabe,

Bewertungen in aggregierter Form erst zu veröffentlichen, wenn mehr als zehn Bewertungen vorliegen. Wir meinen, dass damit ein ausgewogenes Bewertungsportal zustande kommt, das die Rechte der bewerteten Ärzte in angemessener Form wahrt.

Was ist zu tun?
Bei datenschutzrechtlich kritischen Vorhaben wie dem Aufsetzen von Bewertungsportalen ist es wichtig, die rechtlichen Vorgaben genau einzuhalten. Eine Beratung durch das ULD oder andere Datenschutzaufsichtsbehörden ist insofern hilfreich.

4.7 Wissenschaft und Bildung

4.7.1 Vermittlung von Medienkompetenz – mit dem ULD

Wenn junge Menschen das Internet nutzen und sich in sozialen Netzwerken tummeln, sind ihnen oft die damit verbundenen Gefahren für ihre persönlichen Daten nicht bewusst. Das ULD versucht durch Vorträge in Schulen und durch Broschüren, Schülerinnen und Schülern den sorgsamen Umgang mit ihren Daten zu vermitteln.



Als das Bildungsministerium vor zwei Jahren die **Initiative Netzwerk Medienkompetenz** startete, um Schülerinnen und Schüler, Lehrkräfte und Eltern über den richtigen und sorgsamen Umgang mit elektronischen Kommunikationsmedien aufzuklären, sind wir dieser Initiative sofort beigetreten. Gemeinsam mit der Verbraucherzentrale Schleswig-Holstein, der Landespolizei, dem Offenen Kanal und anderen Organisationen führt das ULD seither Veranstaltungen an Schulen in Schleswig-Holstein durch. Dabei kommt die vom ULD herausgegebene Jugendbroschüre „Entscheide DU – sonst tun es andere für Dich!“ zum Einsatz (32. TB, Tz. 4.7.1).

Ergänzt wird dies zukünftig durch einen **gemeinsamen Internetauftritt**, über den von Schulen oder auch von den Schülerinnen und Schülern Informationen und Materialien abgerufen werden können. Wir meinen, dass sich der personelle und zeitliche Aufwand lohnt. Die Jugendlichen werden zum Nachdenken veranlasst und gehen vorsichtiger mit persönlichen Daten im Internet um.

Was ist zu tun?
Wir werden das Netzwerk Medienkompetenz weiter tatkräftig unterstützen.

4.7.2 Elektronische Lernplattformen und der Datenschutz

Die Schulen setzen zunehmend für organisatorische Zwecke, für die Kommunikation zwischen Lehrern und Schülern und für die Verteilung von Unterrichtsmaterial verschiedene elektronische Verfahren ein. Diese als „Lernplattformen“ oder „digitale Lehrerzimmer“ bezeichneten Verfahren müssen mit dem Datenschutz in Einklang stehen.

Lernplattformen wie InfoMentor, lo-net[2], Fronter oder Moodle sollen für eine breitere und schnellere Kommunikation zwischen Schülerinnen und Schülern, Eltern, Lehrkräften und Schulleitungen sorgen. Diese sind nicht nur für die Kommunikation und die schulische Organisation nützlich, sondern auch für den Austausch schulischer Aufgaben von Lehrkräften mit Schülerinnen und Schülern. Dabei werden personenbezogene Daten verarbeitet. Einige dieser Plattformen werden von privaten Anbietern kostenfrei auf deren Servern angeboten. Infrage steht somit auch dort die sichere Speicherung der Daten.

Das Bildungsministerium hat bisher keine regelnden Empfehlungen für die Schulen getroffen, ob und wenn ja welche Angebote wie verwendet werden dürfen. Das ULD wird zunehmend von Schulleitungen wegen der Einhaltung des Datenschutzes befragt, zumeist aber erst, wenn diese Plattformen bereits genutzt werden. Wegen der **Komplexität und der Unterschiedlichkeit** der Anwendungen können keine einheitlichen Aussagen getroffen werden. Jedes Produkt muss separat auf den Datenschutz hin geprüft werden. Diese Prüfung erfolgt in der Regel nicht, wie es nötig wäre, durch die Schulleitungen. Datenschutzverstöße sind so vorprogrammiert.

Was ist zu tun?
Das Bildungsministerium sollte zeitnah Regelungen für den Einsatz solcher Plattformen treffen. Das ULD ist bereit, für den Einsatz in Schulen vom Bildungsministerium freigegebene Anwendungen verbindlich zu prüfen.

4.7.3 LanBSH und geplanter USB-Stick erhöhen Datensicherheit

Die Einführung des Landesnetzes Bildung Schleswig-Holstein bringt durch eine standardisierte IT-Konzeption Arbeitserleichterungen für die Schulverwaltungen und erhöht das Sicherheitsniveau. Solche technischen Konzepte fehlen jedoch noch bei der Verarbeitung von Schülerdaten durch die Lehrkräfte.

Die Lehrkräfte sind oft gezwungen, personenbezogene Daten ihrer Schülerinnen und Schüler im häuslichen Bereich **mithilfe privater Rechner** zu verarbeiten. Automatisierte Zeugniserstellungen setzen den Einsatz elektronischer Datenverarbeitung (EDV) voraus. Lehrer-EDV-Arbeitsplätze in der Schule fehlen. Viele Lehrkräfte haben zudem immer noch Bedenken, die Genehmigung zur häuslichen elektronischen Datenverarbeitung bei den Schulleitungen einzuholen. In aus diesen Unsicherheiten entstandenen Konflikten zwischen Lehrkräften und Schul-

leitungen muss das ULD immer wieder vermitteln, die Rechtsgrundlagen erklären und technische Lösungen erläutern.

Das Institut für Qualitätssicherung an Schulen Schleswig-Holstein (IQSH), das mit dem ULD bei der Konzeptionserstellung und beim Aufbau des Landesnetzes Bildung Schleswig-Holstein (LanBSH) eng zusammenarbeitet, hat eine technische Lösung entwickelt, die die Datensicherheit der im häuslichen Bereich der Lehrkräfte verarbeiteten personenbezogenen Daten erhöht und den Lehrkräften die Unsicherheit hinsichtlich des Datenschutzes nehmen kann. Gedacht ist an eine ausschließliche Nutzung wirksam **verschlüsselter USB-Sticks**, die vom Schulträger beschafft und von den Schulleitungen an jede Lehrkraft ausgegeben werden und die einheitlich konfiguriert sind. Die mittlerweile hohen Speicherkapazitäten dieser USB-Sticks ermöglichen es, dass die im häuslichen Bereich verarbeiteten Daten ausschließlich darauf gespeichert werden. Die Verschlüsselung minimiert das Risiko, dass Unbefugte Kenntnis von den personenbezogenen Daten nehmen. Den Schulleitungen wird so zudem ermöglicht, im Rahmen der Fachaufsicht zu kontrollieren, ob die Regelungen der Datenschutzverordnung Schule zum Umfang und zur Löschung der von den Lehrkräften mit Genehmigung verarbeiteten personenbezogenen Daten eingehalten werden.

Was ist zu tun?
Das Bildungsministerium sollte eine solche technische Lösung flächendeckend in den Schulen des Landes einführen.

4.7.4 Schulleiterfortbildungen im Datenschutz weiterhin erforderlich

Schulleiterfortbildungen des IQSH in Kooperation mit dem ULD sind aus Zeitgründen nur begrenzt attraktiv. Den Schulleiterinnen und Schulleitern kann – trotz steigender Anforderungen – nur Grundwissen vermittelt werden.

Schulleiterinnen und Schulleiter sind nach der Datenschutzverordnung Schule für die ordnungsgemäße und datenschutzkonforme Verarbeitung der personenbezogenen Daten der Schülerinnen, Schüler und Eltern verantwortlich. Es gibt eindeutige Rechtsvorschriften im Schulgesetz und in der Datenschutzverordnung Schule. Eingaben von Eltern und Anfragen von Schulleitungen weisen aber auf **Wissens- und Umsetzungsdefizite** hin. Das ULD und das IQSH als Fortbildungsinstitut für die Lehrkräfte versuchen dauernd, diese Lücken teilweise aufzufüllen. Allerdings konnten nur Kurse an zwei Nachmittagen angeboten werden, weil für die Schulleiterinnen und Schulleiter „jede Stunde zählt". Bei diesen bis in die späten Abendstunden hineingehenden Kursen kann den Schulleitungen nur ein begrenzt ausreichendes Basiswissen zum Datenschutz und dessen Umsetzung vermittelt werden. Aus Sicht des ULD wäre eine Ausweitung auf eine zweitägige Schulungsveranstaltung, gern auch vor Ort, wünschenswert, um das nötige Datenschutzrüstzeug vermitteln zu können.

Was ist zu tun?
Das Bildungsministerium sollte es dem IQSH ermöglichen, in Kooperation mit dem ULD den Schulleitungen Zweitagesveranstaltungen als Datenschutzfortbildungen anzubieten.

4.7.5 Schulen brauchen ein einheitliches und nachhaltiges Datenschutzkonzept

Eine große Anzahl von Schulen ist bezüglich des Datenschutzes schlecht aufgestellt. Durch den Einsatz schulischer Datenschutzbeauftragter kann eine Verbesserung erreicht werden.

An die Arbeit von Schulverwaltungen kann realistischerweise nicht derselbe strenge Maßstab wie bei „normalen“ Verwaltungen angelegt werden. Gefordert bleibt aber die Beachtung der datenschutzrechtlichen Vorgaben. Trotz verstärkter Schulungsmaßnahmen, etwa von Schulräten und auf Schulleiterdienstversammlungen, stellt das ULD in den Schulen oft stark **voneinander abweichende Praktiken** fest, bei denen Datenschutzvorschriften verletzt werden. Das Problem lässt sich teilweise dadurch beheben, dass vom Bildungsministerium für das Datenschutzkonzept Vorgaben gemacht werden. Wir haben hierfür konkrete Vorschläge erarbeitet und Hilfe bei der Umsetzung angeboten.

Zwei berufsbildende Schulen, die jeweils einen schulischen Datenschutzbeauftragten hatten, fusionierten zu einem **regionalen Bildungszentrum**. Anlässlich der Fusion entwickelten sie ein Datenschutzkonzept, um die Regelungen des Schulgesetzes und der Datenschutzverordnung Schule in den schulischen Alltag praktikabel zu integrieren. Das Konzept wird von der Leitung des regionalen Bildungszentrums in Kraft gesetzt und ist somit von allen Lehrkräften zu beachten.

Diese Initiative der **schulischen Datenschutzbeauftragten** zeigt den Mehrwert einer solchen Institution, insbesondere für die Schulleitungen, die deren Arbeit ernst nehmen und ausreichend Zeit zur Verfügung stellen. Während die berufsbildenden Schulen bereits seit einem Jahrzehnt schulische Datenschutzbeauftragte bestellen müssen, ist dies für die allgemeinbildenden Schulen keine Verpflichtung. Das ULD wirbt seit Jahren für die Bestellung behördlicher bzw. schulischer Datenschutzbeauftragter, bei den allgemeinbildenden Schulen bisher aber nur mit begrenztem Erfolg.

Was ist zu tun?
Das Bildungsministerium sollte im Rahmen seiner Möglichkeiten stärker für die Bestellung schulischer Datenschutzbeauftragter bei den Schulleitungen werben und den Schulen konzeptionelle Vorgaben beim Datenschutz machen.

4.7.6 Fehlende Umsetzung einer Meldevorschrift

Die Umsetzung der Meldepflicht von allgemeinbildenden zu berufsbildenden Schulen führt wegen des Fehlens einer technischen Lösung zu bürokratischem Mehraufwand.

> **?** ***§ 30 Abs. 7 Schulgesetz***
>
> *Die Vorschrift verlangt von den allgemeinbildenden Schulen und den Förderzentren, dass sie die Schülerinnen und Schüler, die diese Schulen verlassen, an die berufsbildenden Schulen melden.*

Um sicherzustellen, dass minderjährige Schülerinnen und Schüler, die allgemeinbildende Schulen oder Förderzentren verlassen, ihrer Berufsschulpflicht nachkommen, übermitteln diese Schularten die Daten der Abgänger an die in ihrem Einzugsbereich befindlichen berufsbildenden Schulen – derzeit in papierener Form oder per unverschlüsselter E-Mail. An Schulstandorten mit mehreren berufsbildenden Schulen erfolgt ein relativ aufwendiges Abgleichverfahren, um festzustellen, ob alle Schülerinnen und Schüler tatsächlich bei den berufsbildenden Schulen ankommen.

Das IQSH hat, beraten vom ULD, eine **technische Lösung** vorgeschlagen. Dessen Umsetzung scheiterte bisher daran, dass das Bildungsministerium noch keine Entscheidung getroffen hat. Die Lösung im Landesnetz Bildung Schleswig-Holstein hat nicht nur verwaltungsökonomische Vorteile, sondern erhöht auch die Sicherheit der zu übermittelnden personenbezogenen Daten.

Was ist zu tun?
Das Bildungsministerium sollte zeitnah eine Entscheidung für die vom IQSH angedachte technische Lösung treffen.

4.7.7 Schulsozialarbeit – eine prinzipiell gute Sache

In der Schulsozialarbeit besteht oft Unsicherheit, ob im Rahmen ihrer Tätigkeit erlangte personenbezogene Informationen weitergegeben werden dürfen.

In vielen Schulen Schleswig-Holsteins sind Schulsozialarbeiterinnen und Schulsozialarbeiter tätig, zumeist mit staatlicher Anerkennung als Sozialarbeiter oder Sozialpädagogen. Deren Arbeit in den Schulen setzt einen vertrauensvollen Umgang mit den ihnen von Schülerinnen und Schülern anvertrauten Informationen voraus. Oft ist im Interesse der Schülerinnen und Schüler aber auch ein Austausch mit den Lehrkräften, den Schulleitungen und anderen Stellen erforderlich. Schulsozialarbeiter verrichten ihre Arbeit zwar in den Schulen, gehören diesen aber organisatorisch nicht an. Sie sind bei den verschiedensten Stellen – etwa beim Schulträger, beim öffentlichen Jugendhilfeträger oder beim Kinderschutzbund – beschäftigt. Oftmals entstehen Unsicherheiten beim **Umgang mit den vertraulichen Informationen**, was zu Reibungen bei der an sich notwendigen Kommunikation mit den Schulleitungen oder Lehrkräften führen kann. Um dies-

bezüglich Hilfestellungen zu geben, werden derzeit in Zusammenarbeit mit dem Sozialministerium und dem Bildungsministerium Hinweise für eine datenschutzgerechte Verarbeitung der von den Schulsozialarbeitern gespeicherten personenbezogenen Daten entwickelt.

Was ist zu tun?
Die Hinweise sollten fertiggestellt, abgestimmt und in die Praxis umgesetzt werden.

4.8 Steuerverwaltung

4.8.1 Grunderwerbssteuer – Verwendung eines Fragebogens

Steuerformulare sind so zu gestalten, dass nicht mehr Daten als erforderlich erhoben werden. Anderenfalls muss darauf hingewiesen werden, wie weit die Auskunftspflicht geht.

Petenten beschwerten sich über einen Fragebogen eines Finanzamtes zur Ermittlung der Grunderwerbssteuerpflicht. Darin wurde nach der Bebauung des Grundstücks, nach **Vereinbarungen mit dem Grundstücksveräußerer**, nach der Art des Grundstücksangebots und nach der Baugenehmigung gefragt. Mussten die angeschriebenen Personen die Fragen alle beantworten? Die gesetzliche Auskunftspflicht besteht nur für Angaben, die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlich sind.

Die Bemessung der Grunderwerbssteuer hängt maßgeblich davon ab, ob bezüglich der Bebauung und des Grundstücks **ein Vertrag oder getrennte Verträge** geschlossen wurden. Besteht ein einheitliches Vertragswerk, so fällt Grunderwerbssteuer für beide Leistungsgegenstände an. Zur Ermittlung der Steuerpflicht ist dabei von Bedeutung, welche Personen auf der Veräußerungsseite stehen, z. B. Bauunternehmer, Makler, Bevollmächtigte oder Treuhänder, und inwiefern diese personell, wirtschaftlich oder gesellschaftlich miteinander verbunden sind. Hängen die Vorgänge voneinander ab, indem etwa der Käufer das Grundstück nur erhält, wenn er auch das zu errichtende Gebäude erwirbt, so können Anhaltspunkte für eine wirtschaftliche Verflechtung und damit für ein einheitliches Vertragswerk vorliegen. Der Fragebogen war nicht zu beanstanden, da darin für den Fall fehlender Bebauungsabsicht darauf hingewiesen wurde, dass keine Auskunftspflicht besteht. Die Fragen zur steuerlichen Ermittlung, z. B. zu den Angeboten des bauausführenden Unternehmens oder des Grundstücksveräußerers, erwiesen sich als geeignet und erforderlich.

Was ist zu tun?
Fragebögen sind so zu gestalten, dass nur die zur steuerlichen Ermittlung erforderlichen Auskünfte eingeholt werden.

4.8.2 Mitgliedsdaten eines Vereins

Bei einer Betriebsprüfung eines gemeinnützigen Vereins kann sich das Finanzamt zur Kontrolle der Mitgliedsbeiträge die Namen und identifizierende Angaben der Mitglieder vorlegen lassen, nicht aber deren Telefonnummern.

Im Rahmen einer Betriebsprüfung forderte ein Finanzamt von einem Verein die Übersendung einer **Mitgliederliste**. Die Liste enthielt neben den Daten der Mitglieder auch Angaben zu den Anschriften und den privaten Telefonnummern der Mitglieder. Die Frage war, inwieweit die Daten zur Erfüllung der Prüfungsaufgaben erforderlich waren. Die Betriebsprüfung sollte insbesondere klären, ob für den Verein die Gemeinnützigkeit erhalten bleibt. Dabei muss die satzungsgemäße Mittelverwendung geprüft werden.

Eine Körperschaft verfolgt gemeinnützige Zwecke, wenn ihre Tätigkeit darauf gerichtet ist, die Allgemeinheit auf materiellem, geistigem oder sittlichem Gebiet selbstlos zu fördern. Die praktizierte Geschäftsführung der Körperschaft muss auf die ausschließliche und unmittelbare Erfüllung der **steuerbegünstigten Zwecke** gerichtet sein und den Bestimmungen entsprechen, die die Satzung über die Voraussetzungen für Steuervergünstigungen enthält. In diesem Zusammenhang prüft die Finanzverwaltung die vollständigen Namen von Mitgliedern eines Vereines und die satzungsgemäße Mittelverwendung, um die Voraussetzungen der Gemeinnützigkeit zu untersuchen.

Die Vollständigkeit der Mitgliedsbeiträge kann nur durch Prüfung der Mitgliederlisten erfolgen. **Erforderlich** ist insoweit die Bekanntgabe von Vornamen und Familiennamen der Mitglieder, Anschrift sowie Datum des Eintritts und gegebenenfalls des Austritts aus dem Verein, nicht jedoch von privaten Telefonnummern.

Was ist zu tun?
Finanzämter müssen bei ihren Prüfungen darauf achten, dass sie nur die erforderlichen Daten erheben.

4.9 Ausländerverwaltung

4.9.1 EU-Bürger im Ausländerzentralregister

Ungeachtet des Grundsatzes der Freizügigkeit innerhalb der Europäischen Union werden Daten über Bürgerinnen und Bürger aus Mitgliedstaaten der Europäischen Union im Ausländerzentralregister entgegen einer Entscheidung des EuGH ebenso gespeichert wie Daten über Drittstaatsangehörige.

Der Europäische Gerichtshof (EuGH) hat Ende 2008 ein Vorabentscheidungsersuchen des Oberverwaltungsgerichts Nordrhein-Westfalen zur Zulässigkeit der Speicherung von Daten über Unionsbürger im Ausländerzentralregister (AZR) dahin gehend beantwortet, dass der Gebrauch eines solchen zentralen Registers

für Unionsbürger nur legitim und mit dem Verbot der Diskriminierung aus Gründen der Staatsangehörigkeit vereinbar ist, wenn das Register zur Unterstützung der mit der **Anwendung aufenthaltsrechtlicher Vorschriften** betrauten Behörden genutzt wird. Die Speicherung von Daten über Unionsbürger zum Zweck der allgemeinen, von der Staatsangehörigkeit unabhängigen Kriminalitätsbekämpfung hat der EuGH dagegen als eine unzulässige Diskriminierung angesehen.

Diese Vorgaben müssen gesetzlich und in der Praxis umgesetzt werden. Das Bundesministerium des Innern legte den **Referentenentwurf eines AZR-Gesetzes** vor, zu dem das ULD Stellung genommen hat.



www.datenschutzzentrum.de/polizei/20100813-stellungnahme-auslaenderzentralgesetz.html

In der Praxis müssen die einschränkenden Vorgaben des EuGH schon heute beachtet werden. Dies gilt für die Beantwortung von behördlichen Auskunftsersuchen an das AZR. Beziehen sich diese auf Unionsbürger, dann darf eine Auskunft nur erteilt werden, wenn sie für spezifische ausländerrechtliche Zwecke benötigt und verwendet wird, in keinem Fall aber für Zwecke der Strafverfolgung. Richten Behörden ihre Auskunftsersuchen schriftlich an die registerführende Stelle, das Bundesamt für Migration und Flüchtlinge (BAMF), so kann dort die Zulässigkeit der Auskunftserteilung im konkreten Einzelfall geprüft werden. Anders ist die Situation im **automatisierten Abrufverfahren**. Hier nimmt die registerführende Stelle keine Überprüfung vor. Die Verantwortung für die Zulässigkeit der Abrufe und die Einhaltung der Einschränkungen aus der EuGH-Entscheidung obliegt allein der abrufenden Stelle.

In Schleswig-Holstein hat die **Landespolizei Zugang zum AZR** im automatisierten Verfahren zentral über das Landeskriminalamt (LKA). Dort haben wir das Abrufverfahren geprüft. Ausreichende technische und organisatorische Vorkehrungen, die die Einhaltung der rechtlichen Anforderungen gewährleisten, waren nicht getroffen worden. Anweisungen des BAMF zur Durchführung von Abfragen über Unionsbürger sind zwar bekannt, es fehlten aber Vorkehrungen, um deren Einhaltung durch alle abrufberechtigten Mitarbeiter sicherzustellen und diese nachträglich kontrollieren zu können. Insbesondere erwies sich die Protokollierung von Abfragen als lückenhaft (Tz. 4.9.2). Das LKA reagierte umgehend und erließ eine vorläufige Handlungsanweisung zur Umsetzung der EuGH-Entscheidung. Darin werden die abrufberechtigten Mitarbeiter auf die zulässigen Zwecke des Abrufs von Unionsbürgerdaten hingewiesen. Sie werden angewiesen, in der Eingabemaske für die Suchanfrage den Veranlasser der Abfrage anzugeben oder diesen in einem Nachweis zu protokollieren.

Mittlerweile wies das BAMF alle Nutzer des automatisierten Abrufverfahrens darauf hin, dass ein Abruf von Daten über Unionsbürger nur noch mit der **Angabe eines Verwendungszwecks** zur Anwendung aufenthaltsrechtlicher Vorschriften statthaft ist. Der Verwendungszweck ist nach einer Dienstanweisung des LKA in der Suchmaske in dem dafür ursprünglich nicht vorgesehenen Feld „Veranlasser" eingetragen. Durch die Verwendung von Abkürzungen wird sichergestellt, dass auch die Angaben zum Veranlasser noch in das Feld passen.

Was ist zu tun?
Das Ausländerzentralregistergesetz und die Gestaltung des automatisierten Abrufverfahrens müssen zügig geändert werden, damit eine europarechtskonforme Nutzung des Ausländerzentralregisters erfolgt.

4.9.2 Protokollierung der Abrufe aus dem Ausländerzentralregister

Bei der Kontrolle des Abrufverfahrens aus dem AZR sind gravierende Lücken in der Protokollierung der Abrufe deutlich geworden.

Nach dem AZR-Gesetz hat die Registerbehörde bei Abrufen anderer Stellen Aufzeichnungen zu fertigen, aus denen u. a. der Zweck des Abrufs und die für den Abruf verantwortliche Person hervorgehen. Die Angabe des Zwecks ist von grundlegender Bedeutung für eine Kontrolle der Zulässigkeit der Abrufe, nicht nur zur Verhinderung der oben dargestellten unzulässigen Abrufe über Unionsbürger. Im LKA wird eine Eingabemaske für Suchanfragen an das AZR verwendet, die vom INPOL-Land-POLAS-Competence-Center (IPCC) stammt. Ein Feld für die Eingabe eines **Verwendungszwecks** fehlt dort. Genutzt wird hierfür inzwischen ein anderes Feld (Tz. 4.9.1). Dies kann allenfalls eine Übergangslösung sein.

Ähnliches gilt für die Angabe der verantwortlichen Person. Das LKA führt die Abrufe üblicherweise im Auftrag einzelner Polizeibeamter durch, die Kennung der tatsächlich abrufenden Person gibt also keinen Aufschluss über die den Abruf veranlassende Person. Die Suchmaske enthält ein Feld für die Eintragung der **verantwortlichen Person**, das aber nicht als Pflichtfeld ausgestaltet ist. Technisch ist nicht sichergestellt, dass die verantwortliche Person immer angegeben wird. Das LKA hat die abrufberechtigten Mitarbeiter mittlerweile angewiesen, Angaben über die verantwortliche Person zu dokumentieren.

Was ist zu tun?
Die Eingabemaske muss ergänzt werden, um eine den gesetzlichen Anforderungen entsprechende Protokollierung der Abrufe sicherzustellen.

4.9.3 Keine Antwort von der Kreisverwaltung

Auch Ausländerbehörden haben als öffentliche Stellen das Datenschutzrecht zu respektieren und eine Datenschutzkontrolle zu ermöglichen. Dies scheint keine Selbstverständlichkeit zu sein.

Ein Rechtsanwalt wandte sich in einem ausländerrechtlichen Verfahren an das ULD. Als zwei Monate nach unserer **Aufforderung zur Stellungnahme** an die sachbearbeitende Ausländerbehörde ergebnislos verstrichen waren, erinnerten wir unter Fristsetzung und unter Androhung einer datenschutzrechtlichen Beanstandung daran. Auch dieses Schreiben blieb unbeantwortet. Erst auf unsere Beanstandung lange nach Fristablauf reagierte die Kreisverwaltung. Was uns dabei mitgeteilt wurde, war Anlass für eine vertiefte Prüfung.

Was ist zu tun?
Nicht nur das ULD steht Petenten gegenüber in der Pflicht; es ist Pflicht aller an einem Prozess beteiligten Behörden, in angemessener Zeit zu reagieren. Verweigerte Kooperation verursacht nicht nur Ärger, sondern zusätzlichen Aufwand und eventuell Sanktionen.

5 Datenschutz in der Wirtschaft

5.1 Beschäftigtendatenschutz im BDSG

Wenig Licht und viel Schatten finden sich in einem überhastet erarbeiteten Regierungsentwurf.



Nach über 30 Jahren Diskussion über die Notwendigkeit und mögliche Inhalte eines Arbeitnehmerdatenschutzgesetzes und im Angesicht der Vielzahl von Datenschutzskandalen im Beschäftigtenbereich in den Jahren 2008 und 2009 legte die Bundesregierung im August 2010 den Entwurf eines Beschäftigtendatenschutzgesetzes vor. Dies geht auf die Absichtserklärung des Koalitionsvertrages auf Bundesebene von CDU, CSU und FDP vom Herbst 2009 zurück: „Wir setzen uns für eine **Verbesserung des Arbeitnehmerdatenschutzes** ein und wollen Mitarbeiterinnen und Mitarbeiter vor Bespitzelungen an ihrem Arbeitsplatz wirksam schützen.“ Hierfür soll das Bundesdatenschutzgesetz (BDSG) um einen Abschnitt zum Schutz von Beschäftigtendaten ergänzt werden.

So begrüßenswert die Entscheidung der Bundesregierung ist, diese Materie endlich zu regeln, so bedenklich ist der Umsetzungsversuch. Der Entwurf weist handwerkliche Fehler wie auch massive inhaltliche Defizite auf. Die Mängel sind derart gravierend, dass die Intention des Schutzes der Beschäftigten vor dauerhafter Überwachung und Kontrolle **ins Gegenteil verkehrt** wird. Die vorgeschlagenen Regeln für eine Ergänzung des Bundesdatenschutzgesetzes verstoßen teilweise gegen europarechtliche und verfassungsrechtliche Vorgaben und müssen dringend revidiert werden.

> Ein Beschäftigtendatenschutzgesetz darf nicht mit dem Makel der Verfassungs- und Europarechtswidrigkeit verabschiedet werden.

Der Entwurf ermächtigt Arbeitgeber zu umfangreichen Eingriffen in die Persönlichkeits- und Freiheitsrechte der Beschäftigten. Bisher **unzulässige Screening-Maßnahmen** würden bei Inkrafttreten dieses Entwurfs legalisiert werden. In der Vergangenheit als Skandale bekannt gewordene Praktiken würden teilweise zulässig. Bisher eindeutig rechtswidrige und von der öffentlichen Meinung abgelehnte Kontrollmaßnahmen durch Arbeitgeber könnten so flächendeckend Eingang in die Unternehmen finden.

Der Entwurf bleibt hinter den Anforderungen der Praxis an eine wirksame Regulierung zurück. Die Übermittlung von Beschäftigtendaten **innerhalb eines Konzerns** und im internationalen Kontext stellt eine datenschutzrechtliche Herausforderung dar, nicht nur für die Großindustrie. Auch in mittelständischen

Unternehmen gibt es legitime Interessen an einem Datenaustausch und ungenügende Datenschutzsicherungen. Vielen Unternehmen fehlt der nötige eigene rechtliche und technische Sachverstand; hinzu kommt eine große Rechtsunsicherheit, die beseitigt werden sollte. Befugnisse zur Datenübermittlung in Konzernen sollten nicht generell im Datenschutzrecht eingeräumt, sondern spezifisch, z. B. bezüglich Beschäftigtendaten, flankiert werden durch Beteiligungsrechte und die Schaffung ausreichender Transparenz.

Beschäftigtendatenschutz ist sowohl Datenschutz- als auch Arbeitsrecht, was vom aktuellen Entwurf weitgehend ignoriert wird. In dieser Schnittmenge regelungsbedürftig sind ein arbeitsrechtliches Verwertungsverbot unzulässig erhobener Informationen, kollektivrechtliche Normierungsmöglichkeiten, ein kollektives Klagerecht, die Übermittlung von personenbezogenen Daten innerhalb von Konzernen und im internationalen Verkehr, der Rahmen für den Einsatz elektronischer Personalakten, die Heim- und Telearbeit und das in der Praxis an Bedeutung gewinnende Whistleblowing.

Der Entwurf ist geprägt vom grundsätzlichen Argwohn der Arbeitgeber gegenüber ihren Beschäftigten. Das für eine nachhaltige Beschäftigungsbeziehung erforderliche Vertrauen zwischen den Beteiligten wird nicht gefördert. Unter Missachtung des Verhältnismäßigkeitsgrundsatzes werden die Überwachung und die Kontrolle von Beschäftigten durch Arbeitgeber legalisiert. Dies schürt eine **Atmosphäre des Misstrauens**. Bestehende Vertrauensbeziehungen zwischen Arbeitgebern und Arbeitnehmern drohen zugunsten eines Klimas der Überwachung und Bespitzelung verloren zu gehen.

Zweck des Beschäftigtendatenschutzgesetzes sollte sein, innerhalb der Unternehmen Vertrauen seitens der Beschäftigten dafür zu schaffen. Der Schutz ihrer Persönlichkeitsrechte dient zugleich der Umsetzung von Compliance-Anforderungen und der Förderung der Produktivität.

Entgegen anderen Entwürfen sieht der aktuelle Regierungsentwurf eine **Ergänzung des BDSG** vor. Ziel ist scheinbar eine enge Verbindung der allgemeinen datenschutzrechtlichen Regeln mit den Regeln zu Beschäftigungsverhältnissen. Dies wird erkauft mit einer Vielzahl von Nachteilen:

- Beschäftigten und Arbeitgebern wäre ein separates Beschäftigtendatenschutzgesetz besser vermittelbar.
- Die Regulierung im BDSG erschwert die Vermittlung in der Praxis und die praktische Anwendung, z. B. durch Aushang im Betrieb.
- Die Aufnahme von Spezialmaterien ins BDSG fördert die bereits jetzt bestehende Unübersichtlichkeit und Unverständlichkeit des Gesamtgesetzes.
- Die Chance zur einheitlichen Regelung des Personalaktenrechts wird vertan.

Unklar bleibt bisher, inwieweit der Entwurf Arbeitnehmer im öffentlichen Dienst von Ländern und Kommunen erfassen soll. Das ULD legte eine ausführliche Stellungnahme zum Regierungsentwurf vor.



https://www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html

5.1.1 Die Krux mit den Mitarbeiterlisten − Weitergabe von Mitarbeiterdaten an Krankenkassen

Ein Unternehmen forderte von einer Krankenkasse die Erstattung der Kosten einer durch den Betriebsarzt durchgeführten Grippeschutzimpfung bei deren Mitgliedern. Es durfte aber nicht die Daten anderer Betriebsangehöriger übermitteln.

Der Leistungskatalog der Krankenkasse sah eine Erstattung für jedes Mitglied vor. Dem Erstattungsantrag des Unternehmens war aber eine komplette **Liste aller geimpften Mitarbeiter** beigefügt, auch wenn sie bei der angeschriebenen Kasse nicht versichert waren. Es handelte sich um die zusammengefasste Rechnung des Betriebsarztes an die Firma für die gesamte Impfaktion. Die reklamierende Krankenkasse befürchtete zunächst – unbegründet – die Weitergabe der Liste an alle Mitarbeiter zur individuellen Geltendmachung der Erstattungsansprüche. Die Sammlung der einzelnen Erstattungsanträge der Mitarbeiter und deren kollektive Weitergabe an die Krankenkasse verstießen aber auch gegen den Grundsatz der Erforderlichkeit.

Das Unternehmen begründete ihr Vorgehen mit der Reduzierung des eigenen **Verwaltungsaufwands**. Der Charakter als Gesamtrechnung des Betriebsarztes sei bei dem Rechnungsdokument zu bewahren gewesen. Ihm war gar nicht bewusst, dass das Vorgehen zu einer unzulässigen Datenübermittlung an den Leistungsträger führte.

Was ist zu tun?
Unternehmen sollten vor der Übersendung kompletter Arbeitnehmerlisten an Dritte stets prüfen, ob diese auch zum Empfang aller Daten berechtigt sind. Anderenfalls müssen die nicht relevanten mitarbeiterbezogenen Angaben auf der Liste geschwärzt oder anderweitig entfernt werden.

5.1.2 GPS im Firmenfahrzeug – Was tun ohne Betriebsrat?

Für neu zugelassene Fahrzeuge zur Güterbeförderung mit zulässigem Gesamtgewicht von mehr als 3,5 Tonnen sowie Busse mit mehr als neun Sitzen einschließlich des Fahrers ist der Einsatz digitaler Tachografen vorgeschrieben. Die Verwendung zusätzlicher GPS-Geräte ist hiervon nicht erfasst.

In einem Unternehmen kommen elektronische **Fahrtenschreiber** zum Einsatz, mit denen die gefahrene Strecke und die Fahrerdaten nach den gesetzlichen Bestimmungen aufgezeichnet werden. Spezielle Vorschriften verpflichten den Arbeitgeber, die Arbeitszeit der Arbeitnehmer aufzuzeichnen und diese Aufzeichnungen mindestens zwei Jahre lang aufzubewahren. Ferner wird in dem Unter-

nehmen ein Global Positioning System (GPS) eingesetzt, über das die **Standortdaten** für die Empfänger der Lieferungen abrufbar waren, um den jeweiligen Lieferstatus zu ermitteln. Nach den Darlegungen des Unternehmens werden die Standortdaten nicht mit personenbezogenen Fahrerdaten verknüpft. Es erfolge keine Nutzung des Systems zur Mitarbeiterüberwachung.

Gleichwohl lassen sich die Standortdaten aus dem GPS mit den personenbezogenen Fahrerdaten aus den Fahrtenschreibern verknüpfen. Wir forderten das Unternehmen auf, eine Unternehmensregelung zu treffen, die sicherstellt, dass kein Personenbezug hergestellt wird und keine Verhaltens- und Leistungskontrolle von Arbeitnehmern erfolgt. Das Unternehmen kam dem nach. Die Regelung erfolgte nicht als Betriebsvereinbarung, da kein Betriebsrat vorhanden war und zu dessen Einsetzung auch keine gesetzliche Pflicht bestand (32. TB, Tz. 5.6.1).

Was ist zu tun?
Mit GPS kann der Arbeitgeber Leistungskontrollen gegenüber seinen Beschäftigten vornehmen. Die dabei erhobenen Standortdaten sind personenbeziehbar. Für deren Verarbeitung bedarf es einer Rechtsgrundlage. Hierfür kommen Betriebsvereinbarungen, aber auch das allgemeine Gesetz mit einer Selbstbindung des Unternehmens in Betracht.

5.1.3 Friseure unter Kontrolle

Eine Friseurkette stattete Geschäfte mit Videokameras aus, die gleichermaßen Kundinnen und Kunden sowie die Angestellten erfassten. Letztere waren so einer dauerhaften Kontrolle ausgesetzt.

Der Inhaber einer Friseurkette installierte Videokameras. Damit sollten Einbrüche und Diebstähle verhindert werden. Die Videoüberwachung wurde zudem zur Kontrolle des Verhaltens der Mitarbeiter in den verschiedenen Filialen genutzt. So konnte per Anruf aus der Zentrale die Anweisung erteilt werden, freundlicher zu lächeln oder sparsamer zu shampoonieren. Die Mitarbeiter konnten sich während der Arbeitszeit der Erfassung praktisch nicht entziehen. Die Rundumkameras erfassten den ganzen Salon. Eine lückenlose Dauerüberwachung stellt einen absolut unzulässigen schweren Eingriff in das Persönlichkeitsrecht der Mitarbeiter dar. Das ULD beanstandete diese **dauerhafte Mitarbeiterüberwachung** und verlangte den Abbau der Kameras.

Betroffen waren auch die **Kunden**. Diese unterlagen zwar keiner Dauerüberwachung, aber es bestand auch insofern keine Erforderlichkeit. Zur Verhinderung von Diebstahl waren mildere Mittel denkbar. So konnten teure Produkte in abschließbaren Vitrinen aufbewahrt werden, auf die nur ein ausgewählter Mitarbeiter Zugriff hat. Die Friseurkette baute die Videokameras ab.

Was ist zu tun?
Videoüberwachung ist insbesondere im Beschäftigtenbereich kritisch zu hinterfragen. Mitarbeiter dürfen keiner Dauerüberwachung ausgesetzt werden.

5.1.4 Beschäftigtenkontrolle per Video beim Discounter

Die verdeckte Arbeitsplatzvideoüberwachung ist grundsätzlich unzulässig. Maßnahmen zur Verhaltenskontrolle von Beschäftigten sind nur im absoluten Ausnahmefall als letztes Mittel erlaubt. Vorrang haben Maßnahmen der offenen Videoüberwachung.

Wir erhielten Hinweise, dass in mehreren Filialen der Krümet Handelsgesellschaft, einer Discount-Kette, Beschäftigte unzulässig verdeckt per Video überwacht werden. Die heimlich und verdeckt installierten Kameras waren auf öffentlich nicht zugängliche **Büro- und Pausenräume** ausgerichtet. Das Verhalten der Beschäftigten wurde unter Zeitangabe bildlich erfasst. Die mindestens über mehrere Wochen vorgenommenen Aufzeichnungen wurden schwerpunktmäßig unter dem Aspekt der individuellen Leistungserbringung ausgewertet und die stichwortartige Beurteilung in schriftlichen Protokollen festgehalten. Mehrmaliges Nachschminken im Pausenraum, Unterhaltungen der Beschäftigten usw. wurden dem jeweiligen Personal zugeordnet und beispielsweise als „**unproduktiv**“ bewertet.

Die Installation der Videotechnik sowie die Auswertung der Videoaufnahmen wurden durch den Sicherheitsdienstleister VISAKO vorgenommen. Das ULD führte bei beiden Unternehmen **Prüfungen** durch und nahm vorhandene Unterlagen in Augenschein. Mit den verdeckten Videoaufzeichnungen sollten, so die Aussagen, Diebstahlsdelikte verhindert bzw. aufgedeckt werden. Aufgrund der vorliegenden Tatsachen wurde gegen die Krümet Handelsgesellschaft ein Bußgeldverfahren eingeleitet. Auch die Tätigkeit der VISAKO ist Gegenstand unserer Ermittlungen.

Die verdeckte Videoüberwachung greift massiv in das Persönlichkeitsrecht der Beschäftigten ein. Zur Aufdeckung einer Straftat dürfen Aufnahmen nur dann erfolgen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht einer solchen Tat begründen, die Datenerhebung zur Aufdeckung erforderlich ist, keine schutzwürdigen Beschäftigteninteressen entgegenstehen und die Maßnahme nach **Art, Ausmaß und Anlass** verhältnismäßig ist. Dies ist nur sehr selten der Fall. Eine Leistungskontrolle darf durch einen verdeckten Kameraeinsatz in der Regel nicht erfolgen.

Was ist zu tun?
Verdeckte Videoaufnahmen von Beschäftigten bedürfen einer besonderen datenschutzrechtlichen Rechtfertigung. Sie müssen den Ausnahmefall bilden und setzen vor allem voraus, dass eine offene Videoüberwachung nicht zum gleichen Ziel führen würde. Bereits an die Zulässigkeit einer offenen Videoüberwachung sind jedoch hohe Anforderungen zu stellen.

5.2 Scoring

5.2.1 Neue Transparenzpflichten für Auskunfteien

Seit April 2010 sind die Voraussetzungen des Scorings gesetzlich geregelt. Vor allem Auskunfteien führen Scoring durch.

Das ULD hat alle in Schleswig-Holstein ansässigen Auskunfteien aufgefordert, Unterlagen zu ihren Scoring-Verfahren vorzulegen. Unser Vorgehen war abgestimmt mit dem anderer Aufsichtsbehörden. Es soll kontrolliert werden, ob die Auskunfteien die neuen gesetzlichen Vorgaben zum Scoring einhalten. So muss anhand eines Gutachtens belegt werden, dass eingesetzte Scoring-Verfahren eine **wissenschaftliche Grundlage** haben.

Die Einhaltung der neuen **Transparenzvorschriften** ist zur Wahrung der Betroffenenrechte relevant, weshalb wir Musterschreiben zur Auskunftserteilung anforderten. Schon eine erste Sichtung der umfangreichen Unterlagen ergab, dass die Informationen über die beim Scoring verwendeten Datenarten bei allen Unternehmen so allgemein gehalten sind, dass die Betroffenen keine wirksame Plausibilitätsprüfung durchführen können. Die Überprüfung ist noch nicht abgeschlossen.

Was ist zu tun?
Auskunfteien müssen ihre Verfahren vollständig mit den neuen gesetzlichen Vorgaben zum Scoring und zur Transparenz in Einklang bringen.

5.2.2 Keine Extrawurst für die Schufa

Die Schufa beliefert viele Unternehmen in Schleswig-Holstein, insbesondere Banken, mit Scorewerten. Trotzdem wollte sie dem ULD zunächst keine Informationen über ihr Scoring-Verfahren erteilen.

Das ULD nahm das Inkrafttreten insbesondere der neuen Scoring- und Transparenzvorschriften zum Anlass, Prüfungen bei schleswig-holsteinischen Banken durchzuführen. Einige Banken teilten uns mit, dass sie Scorewerte der Schufa nutzen. Über Einzelheiten zu dem **Zustandekommen dieser Werte** konnte aber keine Auskunft gegeben werden, weil die Schufa diese Informationen seinen Geschäftspartnern unter Verweis auf „Geschäftsgeheimnisse" vorenthielt.

Dies ist natürlich kein Argument zur Zurückweisung der datenschutzrechtlichen Kontrollbefugnis des ULD. Da die Schufa Unternehmen in allen Bundesländern mit Scorewerten beliefert, war eine Überprüfung und **Abstimmung im Düsseldorfer Kreis**, dem Zusammenschluss der deutschen Aufsichtsbehörden, in dessen Arbeitsgruppe (AG) Auskunfteien geplant. Kurz vor der anberaumten Sitzung der AG Auskunfteien strengte die Schufa ein gerichtliches Eilverfahren gegen die für die Schufa zuständige hessische Datenschutzaufsichtsbehörde an. Ziel war es, die Offenbarung der Details zu den Scoring-Verfahren der Schufa an andere Aufsichtsbehörden zu verhindern. Die Schufa berief sich auf Betriebs- und Geschäftsgeheimnisse.

Das ULD forderte daraufhin direkt von der Schufa die Bereitstellung der Informationen zum Scoring, das von schleswig-holsteinischen Unternehmen genutzt wird. Wir wollten wissen, weshalb diese Informationen, die zur Wahrnehmung der Datenschutzpflichten nötig sind, nicht an die schleswig-holsteinischen Vertragspartner weitergegeben werden. Die Schufa verweigerte die Bereitstellung und lud stattdessen das ULD wie auch andere Aufsichtsbehörden zur **mündlichen Unterrichtung** in Einzelterminen nach Wiesbaden ein und verlangte zugleich die Unterzeichnung einer Vertraulichkeitserklärung durch die Teilnehmenden. Dieser Vorschlag wurde nicht nur vom ULD abgelehnt.

Mit diesem Vorgehen lief die Schufa sehenden Auges Gefahr, dass das ULD die Unternehmen im Land darüber unterrichtete, dass Schufa-Scoring-Verfahren nicht eingesetzt werden könnten, da für diese die Datengrundlage nicht hinreichend transparent ist. Eine ganze Reihe von Datenschutzaufsichtsbehörden forderte nun von der Schufa die direkte Auskunftserteilung, auch unter Hinweis auf die für sie geltende gesetzliche Verschwiegenheitspflicht. Die Schufa muss, ebenso wie andere bundesweit agierende Unternehmen, ein Interesse an einer Abstimmung der Aufsichtstätigkeit haben, zumal aufsichtsbehördliche **Mittel gegen die Vertragspartner der Schufa** im Raum stehen.

Zum Einsatz dieser Mittel kam es dann vorläufig nicht. Die Schufa stellte dem ULD wie auch anderen Aufsichtsbehörden Unterlagen zu ihren Scoring-Verfahren zur Verfügung. Sie teilte mit, dass sie die Frage der Erörterung von Betriebs- und Geschäftsgeheimnissen im Düsseldorfer Kreis in einem gerichtlichen Hauptsacheverfahren klären lassen wolle. Zuletzt erfolgte in einer Sitzung der AG Auskunfteien des Düsseldorfer Kreises im November 2010 eine **Erläuterung der vorgelegten Unterlagen** durch die Schufa gegenüber allen teilnehmenden Aufsichtsbehörden.

Was ist zu tun?
Schleswig-holsteinische Unternehmen müssen gegenüber dem ULD genaue Auskünfte zu den von ihnen durchgeführten Datenverarbeitungsverfahren geben können. Bedienen sich Unternehmen Verfahren anderer Stellen, müssen sie auch darüber genaue Auskünfte erteilen können.

5.3 ELV – unwirksame Kassenbon-Einwilligungen

Die langen Kassenzettel beim Zahlen im Elektronischen Lastschriftverfahren in Supermärkten und Tankstellen gerieten ins Visier der Datenschutzbehörden. Es wurde nachgefragt, was mit den Zahlungsdaten der Kunden passiert.

Handelsunternehmen in Schleswig-Holstein setzen das sogenannte **Elektronische Lastschriftverfahren** (ELV ein, wenn Kunden an der Kasse per EC-Karte zahlen. Dabei unterschreibt der Kunde auf dem Kassenbon mit einer Einzugsermächtigung, dass der Betrag von seinem Konto abgebucht werden darf. Zudem befreit er seine Bank vom Bankgeheimnis, falls die Lastschrift „platzt“; dann ist von einer Rücklastschrift die Rede. Dies passiert z. B., wenn das Konto nicht ausreichend gedeckt war. Die Bank darf dann die Adresse des Kunden an den Supermarkt weitergeben, damit dieser die offene Forderung eintreiben kann.

Mit der Zeit wurden die Klauseln auf den Kassenzetteln immer länger, was Verbraucher- und Datenschützer veranlasste, sie genauer unter die Lupe zu nehmen. Schon länger ist bekannt, dass einzelne Händler eigene schlechte Zahlungserfahrungen speichern. Wenn eine Rücklastschrift bei einem Händler einging, erfolgte eine Speicherung in einer sogenannten **Sperrdatei** dieses Händlers. Dieses Vorgehen ist zulässig, solange die Forderung nicht beglichen ist. Der Händler hat ein berechtigtes Interesse daran, den Kunden nicht noch mal im „riskanten“ Lastschriftverfahren bezahlen zu lassen. Denn die Gefahr ist hoch, dass das Konto noch immer nicht gedeckt ist. Außerdem dürfen Händler auch Kartenverlustmeldungen aus einem polizeilichen Register, der KUNO-Datei, verwenden.

Will ein Händler das Lastschriftverfahren nicht einsetzen, bleibt im Wesentlichen die Möglichkeit der Barzahlung oder des **EC-Cash-Verfahrens**. Bei letzterem wird ebenfalls die EC-Karte eingesetzt, allerdings in Kombination mit der PIN. Dieses Verfahren ist für den Händler sicherer als das ELV, da dieser bei erfolgreicher Autorisierung der Zahlung von der Bank des Kunden eine Zahlungsgarantie erhält. Diese Zahlung kann also nicht mehr „platzen“. Dafür berechnen die Banken den Händlern allerdings Gebühren.

Die meisten Händler bedienen sich sogenannter EC-Netzbetreiber. Diese stellten ursprünglich nur die Kartenlesegeräte zur Verfügung, leiteten die Zahlungsdaten weiter und wickelten die Zahlung ab. Das Leistungsangebot der EC-Netzbetreiber wurde nun sukzessive erweitert. Hintergrund war der Wunsch der Händler, das teure PIN-Verfahren zu vermeiden und das zunächst unentgeltliche ELV zu nutzen, allerdings möglichst ohne das Risiko von Rücklastschriften. Entwickelt wurden Instrumente zur **Risikomessung, -steuerung und -übernahme**.

Die EC-Netzbetreiber entwickelten das Instrument der sogenannten **Zahlungswegeempfehlung**. Wird aus Sicht der EC-Netzbetreiber eine „riskante EC-Karte“ eingesetzt, bei der aus bestimmten Gründen ein Rücklastschriftrisiko besteht, wird nicht das ELV eingesetzt. Vielmehr wechselt die Kasse zum teureren, aber sicheren PIN-Verfahren. Um das Risiko einschätzen zu können, sammeln die EC-Netzbetreiber zentral von verschiedenen Händlern Informationen über Rücklastschriften. Außerdem werden Datum, Uhrzeit, Ort und Betrag jeder Zahlung im Lastschriftverfahren gespeichert. Anhand dieser Informationen werden u. a. sogenannte Händlerlimits berechnet. Mithilfe dieses Limits kann ein Händler z. B. bestimmen, dass das ELV nur eingesetzt wird, wenn verschiedene Einkäufe mit einer EC-Karte in einem Zeitraum von 30 Tagen einen Betrag von 400 Euro nicht übersteigen.

Die Datenschutzbehörden bemängeln, dass die Kundinnen und Kunden **nicht ausreichend informiert** werden. In vielen Fällen erfolgt kein Hinweis, was mit den Zahlungsdaten über die herkömmliche Nutzung im ELV hinaus passiert. Wenn ein Hinweis auf den Kassenzettel gedruckt war, so oftmals nur auf dem Exemplar des Händlers. Dem Kunden wurde der Hinweis nicht zur eingehenden Information überreicht. In der eiligen Kassensituation hat er auch faktisch keine Möglichkeit, sich einen langen Text vor der Unterschrift in Ruhe durchzulesen.

Die Hinweise auf den Kassenzetteln sind weiterhin sehr pauschal und für den Kunden nicht verständlich. Nach Ansicht des ULD kommt die **Einwilligung mit der Unterschrift** nach dem Auslesen der Karte und erfolgten Datenabgleich mit den Listen der EC-Netzbetreiber auch zu spät. Die Überprüfung und Bewertung der Vorgänge bei den EC-Netzbetreibern ist noch nicht abgeschlossen. Es gab Hinweise, dass die Daten aus dem ELV für andere Zwecke als nur für die der Zahlungsabwicklung genutzt wurden. Zwei Datenschutzaufsichtsbehörden stellten Strafanträge wegen des Verdachts der unzulässigen Datenweitergabe zu Zwecken der Zahlungsverkehrsanalyse.

Was ist zu tun?
Sämtliche Verfahren der EC-Netzbetreiber gehören auf den Prüfstand. Händler und EC-Netzbetreiber müssen ihre Kunden umfassend und verständlich darüber informieren, was mit den Zahlungsdaten passiert.

5.4 Bonitätsabfragen durch die Wohnungswirtschaft

Vermieter holen vor der Vermietung von Wohnraum zu den Mietinteressenten nicht selten Informationen über Auskunfteien ein. Für derartige Bonitätsabfragen bestehen datenschutzrechtliche Grenzen.

Das ULD hat bei 53 Unternehmen der Wohnungswirtschaftsbranche eine Befragung zur Praxis der Bonitätsabfragen zu Mietinteressenten durchgeführt. Es wurde gebeten, die verwendeten Formulare vorzulegen und zu erläutern, welche Auskünfte bei Auskunfteien eingeholt werden. Aus den Antworten ergibt sich, dass Angaben zur Bonität vorwiegend nur zum **letztverbleibenden Mietinteressenten** eingeholt werden.

Aus Datenschutzsicht darf eine Auskunft zu einem Mietinteressenten tatsächlich erst dann eingeholt werden, wenn der Abschluss des Mietvertrages mit diesem Bewerber nur noch vom positiven Ergebnis der Bonitätsprüfung abhängt. Da der Vermieter mit dem Abschluss des Mietvertrages das Risiko eingeht, dass ein Mieter wegen Zahlungsunfähigkeit oder -unwilligkeit den Mietzins nicht begleicht, hat der Vermieter bei einem finanziellen Ausfallrisiko grundsätzlich ein **berechtigtes Interesse** an einer Bonitätsauskunft. Dieses besteht noch nicht bei einer zeitgleichen Datenabfrage zu mehreren Wohnungsinteressenten.

Was ist zu tun?
Nur zum letztverbleibenden Bewerber darf eine Bonitätsauskunft eingeholt werden. Erst wenn diese Auskunft zu einem negativen Ergebnis führt, darf eine Auskunft zum Bewerber erfolgen, der in der Rangliste folgt.

5.5 Datenschutz in der Versicherungswirtschaft

Die Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises verhandelt mit dem Gesamtverband der Deutschen Versicherungswirtschaft unter Vorsitz des ULD über einen großen Strauß von Datenschutzfragen der Branche.

Die Arbeitsgruppe (AG) erstellte eine Stellungnahme zu Bonitätsprüfungen in der Versicherungswirtschaft. Die Verhandlungen zur Erstellung einer Schweigepflichtentbindungs- und datenschutzrechtlichen Einwilligungserklärung mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) sind weit fortgeschritten. Das neue Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) soll im April 2011 in Form einer Auskunftei in Betrieb gehen.

- **Bonitätsabfrage und Scoring bei Versicherungen**

Die Datenschutzaufsichtsbehörden in der AG Versicherungswirtschaft gaben zur Frage der **Zulässigkeit von Bonitätsabfragen** durch Versicherungsunternehmen eine Stellungnahme gegenüber dem GDV ab. Danach darf ein Versicherungsunternehmen Bonitätsauskünfte nur einholen, wenn in dem konkreten Einzelfall ein berechtigtes Interesse an der Information dargelegt werden kann. Schutzwürdige Interessen der betroffenen Person dürfen dem nicht entgegenstehen. Entscheidend ist, ob der Vertrag für das Unternehmen ein sogenanntes **finanzielles Ausfallrisiko** birgt.

Ein finanzielles Ausfallrisiko sieht die AG Versicherungswirtschaft nur bei ganz **bestimmten Versicherungsarten** für gegeben. Ein solcher Sonderfall sind Kreditversicherungen, bei denen das Versicherungsunternehmen die Rolle eines Bürgen einnimmt. Bei Pflichtversicherungen, bei denen aufgrund gesetzlicher Regelungen die Aufrechnung fälliger Prämienforderungen gegenüber einem begünstigten Dritten ausgeschlossen ist, kann das Ausfallrisiko auch eine Bonitätsanfrage legitimieren. Für die Krankenvollversicherung im Basistarif wurde für die Fälle, in denen eine gesetzliche Verpflichtung zur Gewährung von Versicherungsverträgen besteht, festgestellt, dass kein berechtigtes Interesse besteht. Für Krankenvollversicherungen außerhalb des Basistarifs wird ein berechtigtes Interesse anerkannt, soweit die abgefragten Daten nicht über den Datenkatalog der Schuldner- und Insolvenzverzeichnisdaten hinausgehen. In Anbetracht der existenziellen Bedeutung von Krankenversicherungsverträgen stehen jeder weiter gehenden Datenabfrage schutzwürdige Interessen des Betroffenen entgegen.

Die rechtliche Bewertung des **Scorings** bei Versicherungsunternehmen befindet sich in der AG noch in der Abstimmung.

- **Einwilligungs- und Schweigepflichtentbindungserklärung**

Die Mustererklärungen zur datenschutzrechtlichen Einwilligung und zur Schweigepflichtentbindung wurden zwischen dem GDV und den Datenschutzaufsichtsbehörden weitgehend abgestimmt (32. TB, Tz. 5.2). Einzelbereiche wie die **Datenweitergabe an Rückversicherer** sowie die Datenweitergabe an Vermittler

bedürfen einer separaten Klärung. Es ist vorgesehen, den abgestimmten Kern der Mustererklärungen 2011 durch den Düsseldorfer Kreis bestätigen zu lassen.

- **Hinweis- und Informationssystem der Versicherungswirtschaft (HIS)**

Ein Unternehmen der informa Unternehmensberatung soll ab April 2011 das neue HIS in Ausgestaltung einer Auskunftei betreiben (32. TB, Tz. 5.2). Dafür wurde eine eigene Gesellschaft, die **Informa Insurance Risk and Fraud Prevention GmbH** (IIRFP) gegründet. Es wurde geklärt, dass über HIS keine Gesundheitsdaten ausgetauscht werden. Weitere Themen der Abklärung zwischen der AG Versicherungswirtschaft, der IIRFP und dem GDV waren die Nutzung des HIS im Leistungsfall in der Lebensversicherung sowie Benachrichtigungs- und Auskunftspflichten insbesondere bei Sachdaten wie Kfz-Daten. Es besteht noch nicht über sämtliche Fragen der Ausgestaltung des neuen HIS Einvernehmen.

5.6 Datenschutz bei Vereinen

Bei der Übermittlung von Mitgliederdaten an einzelne Vereinsmitglieder sind datenschutzrechtliche Vorgaben zu beachten. Die Einschaltung eines Datentreuhänders erweist sich hierbei als suboptimal.

Ein Vereinsmitglied begehrte vom Verein die **Übersendung einer Mitgliederliste**. Ausnahmsweise dürfen Mitgliederdaten ohne die Einwilligung der Betroffenen und bei Fehlen einer Satzungsregelung übermittelt werden, wenn das Vereinsmitglied ein berechtigtes Interesse – etwa ein konkretes Begehren im Rahmen der vereinsinternen Willensbildung – wahrnimmt und keine schutzwürdigen Mitgliederinteressen entgegenstehen. Schutzwürdige Belange stehen der Datenübermittlung bei einer Nutzung für Werbezwecke entgegen. In jedem Fall sind Widersprüche der Mitglieder gegen die Datenübermittlung zu berücksichtigen.

Nicht zu empfehlen ist die **Zwischenschaltung eines Treuhänders**, der etwaige Widersprüche der Vereinsmitglieder gegen eine Übermittlung ihrer Daten entgegennehmen, prüfen und bearbeiten soll. Denn für eine Übermittlung der Mitgliederliste vom Verein an den Treuhänder besteht in der Regel keine Rechtsgrundlage. Der Treuhänder wäre zudem selbst für die Datenverarbeitung verantwortlich und unterläge einer Vielzahl von Pflichten, auch im technischen und organisatorischen Bereich. Der Verein sollte selbst eine Prüfung vornehmen, inwiefern die Mitgliederdaten an ein Vereinsmitglied übermittelt werden dürfen. Er sollte Verfahren einrichten, mit denen eine vom Vorstand unbeeinflusste Willensbildung im Verein möglich ist.

Was ist zu tun?
Der Vereinsvorstand prüft bei Verlangen eines Vereinsmitgliedes auf Übersendung einer Mitgliederliste, ob hierfür Einwilligungen der Mitglieder vorliegen und ob ein konkretes mitgliedschaftliches Begehren dargelegt wurde. Widersprüche der Mitglieder sind zu beachten. Von der Einsetzung eines Treuhänders ist abzuraten.

5.7 Smart Meter

Seit Januar 2010 verpflichtet das Energiewirtschaftsgesetz Energieversorgungsunternehmen, bei Neubauten und Umbauten zur Verbesserung der Energiebilanz sogenannte intelligente Zähler zur Messung der verbrauchten Energiemenge einzubauen bzw. anzubieten.

Der Bundesgesetzgeber verpflichtete die Unternehmen mit Ablauf des Jahres 2010 zum Angebot tageszeitabhängiger und lastvariabler Tarife. Dies sind Tarife, bei denen in Abhängigkeit von der im Netz verfügbaren Energiemenge oder dem Zeitpunkt der Entnahme der Energie die Preise variabel gestaltet sind. Der **verpflichtende Einsatz intelligenter Zähler** beschränkt sich derzeit auf die Messung des Stromverbrauches. Dabei wird es nicht bleiben. Die Einführung dieser Technik ist in sämtlichen Versorgungssparten, also auch Gas und Wasser, geplant und wird in Pilotprojekten getestet.

Zweck der gesetzlichen Vorgaben ist die Verbesserung der Kontrolle und Steuerung des Verbrauchs. Außerdem ist dies der erste Schritt zu sogenannten intelligenten Versorgungsnetzen – Smart Grids. Im Gegensatz zu den herkömmlichen (Ferraris-)Zählern sind die intelligenten Zähler in der Lage, sekundengenau den Verbrauch zu erfassen. Die gemessenen Daten können für **feingranulare Last- und Nutzungsprofile** verwendet werden. Die Auswertung erlaubt sogar die Feststellung, welches Gerät die Energie verbraucht hat.

Die moderne Gesellschaft ist durch eine hochtechnisierte Lebensweise geprägt, die den Verbrauch von Ressourcen mit sich bringt, also von Strom, Gas, Wasser oder Wärmeenergie. Tagesabläufe spiegeln sich in der Nutzung der Ressourcen wider. Mit dem technischen Potenzial der zeitlich kleinteiligen und gerätegenauen Erfassung des Verbrauchs können die Lebensgewohnheiten Betroffener durch intelligente Zähler abgebildet werden. Diese Zählertechnologie birgt somit ein **hohes Ausforschungspotenzial**. Der Eingriff in die Privatsphäre der Betroffenen ist vergleichbar mit der akustischen Wohnraumüberwachung. Sie geht teilweise darüber hinaus. Der Einsatz intelligenter Zähler berührt nicht nur das Recht auf informationelle Selbstbestimmung. Auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung kann dadurch verletzt werden (32. TB, Tz. 7.3).

Der Gesetzgeber hat bei der Einführung der Zähler die potenzielle Gefährdung für die Persönlichkeitsrechte der Betroffenen **vollständig ignoriert**, obwohl der Bundesrat die Regelung dieses Aspektes im Gesetzgebungsverfahren angemahnt hatte. Einziger Datenschutzmaßstab für die Verarbeitung der Verbrauchsdaten bleibt daher das BDSG. Eine Verwendung der durch intelligente Zähler erhobenen Daten ist nur zulässig, wenn dies zur Erfüllung bestehender Energielieferverträge unbedingt erforderlich ist oder die Betroffenen freiwillig und informiert in die Erhebung, Verarbeitung und Nutzung der Daten eingewilligt haben. Sie können ihre Einwilligung jederzeit widerrufen.

Das ULD fordert wegen des Gefährdungspotenzials für die Privatsphäre der Betroffenen durch die Verwendung detaillierter Nutzungsprofile den Erlass einer spezialgesetzlichen Regelung für die Erhebung, Verarbeitung und Nutzung der durch intelligente Zähler erhobenen Verbrauchsinformationen.

Eine Spezialregelung muss sich am **Zweck der Verarbeitung** der erhobenen Verbrauchsdaten orientieren. Dabei ist zwischen Bestandsdaten, abrechnungsrelevanten Daten und steuerungsrelevanten Daten zu unterscheiden. Bestandsdaten sind Daten, die Auskunft über die Identität des Betroffenen und der Entnahmestelle geben. Sie werden unabhängig vom konkreten Verbrauch durch die Energieversorgungsunternehmen erhoben, verarbeitet und genutzt. Abrechnungsrelevante Daten sind sowohl einzelne als auch aggregierte Verbrauchsinformationen, die Auskunft über die Menge der verbrauchten Energie über einen bestimmten Zeitraum geben. Deren Verarbeitung ist erforderlich, um die vereinbarte Versorgungsleistung abzurechnen. Die Länge des Erfassungszeitraums wird maßgeblich durch die Abrechnungsintervalle des Versorgungsvertrages bestimmt. Steuerungsrelevante Daten ergeben individuelle Verbrauchsprofile mit Angaben über die Netznutzung durch die Betroffenen, zu den die Energie nutzenden Geräten, zur Art des Verbrauchs und weitere für die Abrechnung nicht relevante technische Informationen. Steuerungsrelevante Daten dürfen nur für die Überwachung des ordnungsgemäßen Betriebs des Versorgungsnetzes und zur Sicherstellung der Versorgung der Verbraucher mit der Ressource durch Versorgungsunternehmen und Netzbetreiber verarbeitet werden. Eine darüber hinausgehende Verwendung steuerungsrelevanter Daten kann nur in anonymisierter Form zugelassen werden.

Eine **bereichsspezifische Regel** muss die Transparenz der Datenverarbeitung und die Wahrung der Betroffenenrechte sichern. Durch angemessene technisch-organisatorische Maßnahmen ist gemäß dem Stand der Technik sicherzustellen, dass bei der Übermittlung der Zugriff unberechtigter Dritter ausgeschlossen ist und Daten nicht durch Unbefugte verändert oder gelöscht werden können.

Intelligente Zähler und die geplanten intelligenten **Verteil- bzw. Verarbeitungsnetze** sind Systeme zur automatisierten Verarbeitung personenbezogener Daten. Für sie müssen integrierte Datenschutz- und Managementsysteme konzipiert und aufgebaut werden mit dem Ziel der Sicherstellung der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Transparenz, der Nichtverkettbarkeit und der Intervenierbarkeit selbst in vernetzten, heterogenen und komplexen Systemumgebungen. Über Risikoanalysen, -bewertungen und -behandlungen können national und international Standards und Vorgehensweisen erarbeitet werden. Die 80. Konferenz der Datenschutzbeauftragten hat Anfang November 2010 einen Beschluss zur intelligenten Messung des Energieverbrauchs gefasst, der eine bereichsspezifische Normierung fordert und dafür datenschutzrechtliche Eckpunkte festhält.


http://www.baden-wuerttemberg.datenschutz.de/lfd/konf/2010/11_04_2.htm

5.8 Einzelfälle

5.8.1 Auskunfteien und Gewerbedaten

Zur Beschaffung von nicht allgemein zugänglichen Gewerbedaten müssen Auskunfteien bei den Gewerbeämtern ein rechtliches Interesse an deren Kenntnisnahme darlegen.

Das **Standardformular einer Auskunftei** zur Begründung des Datenbedarfs bei Gewerbeämtern enthielt folgende Formulierung: „Wir benötigen die Angaben für die Beurteilung eines Kreditvertrages bzw. wegen Forderungseinzug.“ Diese Formulierung hat einen doppelten Inhalt: Die „Beurteilung eines Kreditantrages“ bezieht sich auf die Erteilung einer Bonitätsauskunft; beim „Forderungseinzug“ geht es um die Erlangung der Kontaktdaten eines Schuldners zur Realisierung einer Forderung.

Gesetzlich gefordert ist aber ein rechtliches Interesse. Dieses setzt eine **konkrete Rechtsbeziehung** zwischen Antragsteller und dem Gewerbetreibenden voraus. Eine solche Beziehung besteht jedoch nicht ohne Weiteres zwischen Auskunftei und einem Gewerbetreibenden. Kreditverträge schließt ein Gewerbetreibender mit einer Bank, nicht mit der Auskunftei. Aus dem Standardformular ergibt sich nicht, ob ein konkreter Kreditantrag des Gewerbetreibenden vorliegt oder nur eine bloße Konditionenanfrage. Bei einer Konditionenanfrage besteht noch keine konkrete Rechtsbeziehung. Würde die Auskunftei im Auftrag einer Bank tätig, der ein konkreter Kreditantrag eines Gewerbetreibenden vorliegt, wäre eine Auskunft möglich.

Für den Forderungseinzug besteht ein rechtliches Interesse einer Auskunftei nur bei **Erwerb der Forderung**. Sie wird dann nicht als Auskunftei, sondern als Inkassounternehmen tätig. Der Forderungserwerb begründet eine konkrete Rechtsbeziehung. Sollen fremde Forderungen realisiert werden, so kommt es darauf an, ob die Auskunftei vom Gläubiger tatsächlich zum Forderungseinzug und zur Vornahme einer erweiterten Gewerbeauskunft beauftragt wurde.

Was ist zu tun?
Die Auskunftei hat bei Einholung einer Gewerbeauskunft eine Vertragsbeziehung zum Gläubiger glaubhaft darzulegen. Für die Vorbereitung einer Bonitätsbewertung müssen Anhaltspunkte für einen konkreten Kreditantrag des Gewerbetreibenden bestehen.

5.8.2 Traueranzeigen als Quelle für Werbedaten

Ein Bürger bekam kurze Zeit nach dem Tod seiner Mutter unverlangt Werbung eines Steinmetzbetriebes mit konkreten Angeboten zum Kauf eines individuellen Grabsteins für die Verstorbene.

Der Bürger und seine Angehörigen fühlten sich durch diese Werbung unmittelbar nach dem Trauerfall in ihren Gefühlen verletzt. Das Grabsteinunternehmen hatte

systematisch die Traueranzeigen der regionalen und überregionalen Tageszeitungen ausgewertet, die Adressen der Hinterbliebenen unter Zuhilfenahme des Telefonbuches ergänzt und anschließend seinen Grabsteinkatalog versandt. Die Daten stammten aus **allgemein zugänglichen Quellen**.

Im Beschwerdefall lagen zwischen dem Tod der Mutter und dem **Zeitpunkt der Versendung** der Werbepost 15 Tage. Der Bundesgerichtshof hat im April 2010 entschieden, dass Briefwerbung für Grabsteine wettbewerbsrechtlich keine unzumutbare Belästigung der Hinterbliebenen darstellt, wenn sie nach Ablauf einer Frist von zwei Wochen nach dem Todesfall erfolgt. Das ULD schloss sich dem an und vertrat die Auffassung, dass die schutzwürdigen Interessen der Betroffenen durch die Einhaltung einer Wartefrist von zwei Wochen zwischen Todesfall und Zusendung der Werbung ausreichend berücksichtigt wurden.

Der fehlende Hinweis auf das **Widerspruchsrecht** der Betroffenen auf dem Werbeprospekt wurde vom ULD beanstandet. Das Unternehmen zeigte sich zunächst bereit, einen schriftlichen Hinweis auf das Widerspruchsrecht in seine Werbeprospekte aufzunehmen. Inzwischen teilte es uns mit, dass es den unmittelbaren Versand von Werbung an Angehörige nach einem Trauerfall völlig eingestellt habe.

Was ist zu tun?
Die Grabsteinbranche sollte die Trauergefühle der Angehörigen beachten und eine „Schonfrist“ von zwei Wochen zwischen dem Todesfall und der Zusendung von Werbematerial unbedingt einhalten.

5.8.3 Was der Finanzberater alles weiß

Ein selbstständiger Finanzberater in Schleswig-Holstein erhielt von einer Bank detaillierte Kontoinformationen über einen ihrer Kunden und sprach ihn mithilfe der Daten an, um ihm ein Produkt zu verkaufen.

Ein Bankkunde war erstaunt, als ihn ein **selbstständiger Finanzberater** anschrieb. Der Brief enthielt kein allgemeines Werbeschreiben, sondern das ausgefüllte Formblatt „Kündigung einer Spareinlage“. Alle Daten – von Namen, Anschrift und Geburtsdatum über Kontonummer bis zur Höhe der Spareinlage – waren schon eingetragen. Wie konnte der Finanzberater an die Daten des Bankkontos gelangt sein? Dieser war für eine Finanzberatungsgesellschaft tätig, welche ein Tochterunternehmen der kontoführenden Bank war und die Aufgabe des Finanzvertriebs übernahm. Die Finanzberatungsgesellschaft griff hierfür auf viele als selbstständige Handelsvertreter agierende Finanzberater zurück.

Der selbstständige Finanzberater hatte die Kontodaten des Bankkunden von der Finanzberatungsgesellschaft erhalten. Das ULD beanstandete die Nutzung der Kontodaten durch den selbstständigen Finanzberater zu Vertriebszwecken, für die es keine Rechtsgrundlage gab. **Angaben zu Kontobewegungen** sind besonders sensible Daten. Die Abbuchung des Partei- oder Gewerkschaftsbeitrags, einer Spende an den Verein zur Förderung von AIDS-Prävention und die Begleichung

der Rechnung des Lungenspezialisten erlauben beispielsweise tiefe Rückschlüsse auf den Privatbereich des Kontoinhabers.

Viele solche freiberuflichen Außendienstmitarbeiter hatten Zugriff auf Kundendatensätze mit Kontoinformationen. Der für die Bank zuständige Datenschutzbeauftragte Nordrhein-Westfalens verhängte gegen diese ein Bußgeld wegen eines schweren **Verstoßes gegen das Bankgeheimnis**.

Was ist zu tun?
Daten über Kontobewegungen sind besonders sensible Daten. Sie dürfen weder von Handelsvertretern noch von der kontoführenden Bank zu Werbezwecken verwendet werden.

5.8.4 Auskunfts- und Löschpflichten der Banken

Ein unvollständig beantwortetes Auskunftsersuchen eines Bankkunden gegenüber seiner Bank offenbarte, dass Kontaktdaten des Kunden seit über zehn Jahren in einer Interessentendatei gespeichert waren.

Ein „frischer“ Bankkunde hatte seine Bank um Auskunft gebeten, wie seine seit Jahren veralteten E-Mail-Adressen und Faxnummern in seinen Datensatz bei der Bank gelangt waren. Die Serviceabteilung der Bank meinte, er müsse die Kontaktdaten selbst angegeben haben. Eine detaillierte Herkunft der Daten könne nicht nachvollzogen werden. Der Kunde war sicher, dass er die seit Jahren inaktiven Adressen nicht angegeben hatte, und vermutete illegale Datenquellen. Unser Nachhaken und eine gründliche Recherche brachten als Datenquelle eine seit mehr als zehn Jahren bestehende **Interessentendatenbank** hervor. Der Bankkunde hatte sich schon vor zwölf Jahren als Interessent an die Bank gewandt und die inzwischen veralteten Daten angegeben. Es kam damals nicht zu einem Vertragsschluss. Trotzdem blieb er mit seinen Kontaktdaten bis ins Jahr 2010 im System der Bank gespeichert. Der neue Kontakt führte zu einer Verknüpfung der Datensätze und zur Aufnahme der alten Interessentendaten in den aktuellen Datensatz.

Verantwortliche Stellen müssen jederzeit Auskunft über die Herkunft der bei ihnen gespeicherten Daten geben können. Dafür haben sie geeignete Maßnahmen der Eingabekontrolle zu treffen. In einem **Datenschutzmanagement** ist ein geeignetes und effektives Verfahren der Auskunftserteilung vorzusehen. Die im Unternehmen laufenden Verfahren müssen ständig präsent und auf ihre Datenschutzkonformität hin geprüft sein. Eine Datenbank darf nicht zwölf Jahre lang „unbemerkt“ anwachsen. Daten sind zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Speicherung von Interessentendaten ist nur in unmittelbarer zeitlicher Nähe zur Anfrage des Interessenten erforderlich.

Was ist zu tun?
Ein umfassendes Datenschutzmanagement gewährleistet, dass jederzeit über die gespeicherten Daten und deren Herkunft Auskunft gegeben werden kann. Daten dürfen nur so lange gespeichert werden, wie sie für die Erreichung des Zwecks der Speicherung erforderlich sind.

5.8.5 Bank bittet um Rückruf

Das Callcenter einer Bank rief wegen eines Problems im Datenbestand an und bat um Rückruf. Der Angerufene war schon seit drei Jahren kein Kunde dieser Bank mehr.

Ein Bürger teilte mit, das Callcenter einer Bank habe ihn angerufen und ihm mitgeteilt, etwas sei mit seinem Datenbestand nicht in Ordnung. Er solle unbedingt einen bestimmten Kundenberater zurückrufen. Der Angerufene war erstaunt, denn er hatte schon **seit drei Jahren kein Konto mehr** bei dieser Bank. Er vermutete, dass es sich um eine „Werbemasche" handelte. Derartige Vorgänge werden uns immer häufiger mitgeteilt.

Das Verbot der „Cold Calls", also von Werbeanrufen, wenn keine Einwilligung des Angerufenen vorliegt, hat sich mittlerweile herumgesprochen. Unternehmen verschiedener Branchen bitten unter der Angabe fadenscheiniger Gründe um einen Rückruf. Der Abonnentin einer Zeitschrift wurde nach Kündigung des Abos z. B. postalisch mitgeteilt, etwas sei mit der Abbuchung schiefgelaufen. Sie solle deshalb zurückrufen. Beim Rückruf stellte sich heraus, dass man ihr die Verlängerung des Abos anbieten wollte. Dabei handelt es sich um eine unzulässige **Umgehung des „Cold Call"-Verbots**. Kundendaten dürfen von Unternehmen nur verwendet werden, wenn es für die Vertragsabwicklung erforderlich ist. Das Nutzen von Kundendaten zur Umgehung des „Cold Call"-Verbots ist nicht erforderlich und deshalb unzulässig.

Was ist zu tun?
Die telefonische Kontaktaufnahme zu Werbezwecken ist nur mit Einwilligung des Betroffenen zulässig.

5.8.6 Spieglein, Spieglein an der Kasse …

Mehrere besorgte Bürger wandten sich an das ULD und beschwerten sich über Spiegel, die über den Kassen von Supermärkten aufgehängt waren.

Die im Kassenbereich vieler Supermärkte aufgehängten Spiegel sollen den Kassiererinnen in erster Linie einen Blick in die Einkaufswagen der Kunden ermöglichen und dienen so dem Schutz vor Diebstahl. Mehrere besorgte Bürger brachten jedoch ihre Befürchtung zum Ausdruck, durch die aufgehängten Spiegel wäre ein **Ausspähen ihrer PIN-Nummer** beim Bezahlen mit EC-Karte durch hinter ihnen in der Warteschlange stehende Kunden möglich.

Ein tatsächlich erfolgtes Ausspähen der PIN-Nummer wurde zwar in keinem Fall erwiesen, doch konnte das ULD die Befürchtungen im Grundsatz nachvollziehen. Die betroffenen Supermärkte wurden über die vorgetragenen Bedenken informiert und gebeten, die Spiegel abzubauen. Die Märke sind unserer Bitte ausnahmslos gefolgt und haben zeitnah die **Spiegel abmontiert**.

Die Spiegel werden nach unserem Eindruck in den Kassenbereichen ohnehin mehr und mehr durch **moderne Videotechnik** verdrängt. Der Vorteil dieser neuen Technik gegenüber den Spiegeln ist, dass der Bereich der PIN-Eingabetastatur für die EC-Geräte durch gezielte Konfiguration ausgeblendet bzw. geschwärzt werden kann. Damit wird sowohl dem Sicherheitsbedürfnis des Unternehmens hinsichtlich der Verhinderung von Diebstählen als auch dem Bedürfnis der Kunden an der Geheimhaltung der PIN-Nummer genügt. Derartige Kamerasysteme müssen aber tatsächlich so konfiguriert sein und dürfen zudem nicht zur Kontrolle der Leistung und des Verhaltens der Kassiererinnen genutzt werden.

Was ist zu tun?
Betroffene Supermärkte sollten zum Auslesen von PIN-Eingaben geeignete Spiegel in den Kassenbereichen abbauen. Auch eine Videokontrolle der Kassenbereiche muss, z. B. durch Ausblenden der Tastatur der PIN-Eingabegeräte, datenschutzkonform gestaltet sein.

5.8.7 Die Kamera als Waffe gegen den Nachbarn

Dem Ideenreichtum streitender Nachbarn sind keine Grenzen gesetzt. Dabei übernimmt die Videokamera oft die Funktion einer bedrohlichen Waffe.

Das ULD erreichen weiterhin zahlreiche Beschwerden von Bürgern, die sich von ihren Nachbarn mittels Videotechnik verfolgt und bedroht fühlen. Gegenseitige Vorwürfe – etwa angebliche Verschmutzung von Vorgärten mit Hunde- und Katzenkot, absichtliches Einbringen von Unkrautsaat in Ziergärten oder Beschädigung von Kraftfahrzeugen – stehen zumeist im Hintergrund. Der wahre Zweck der Kameras ist zumeist die **Einschüchterung** des ungeliebten Nachbarn.

Bei der Bearbeitung solcher Beschwerden unterscheidet das ULD zwei unterschiedliche Fallgruppen. Sind bei den dargestellten Sachverhalten **öffentliche Belange** berührt, z. B. durch Beobachtung von Bürgersteigen und öffentlichem Straßenraum, fordert das ULD die Kamerabetreiber auf, die Überwachung zu beenden und die Geräte abzubauen. Nötigenfalls werden Bußgeldverfahren wegen unzulässiger Erhebung personenbezogener Daten eingeleitet.

Wird nur **das Nachbargrundstück** beobachtet, verweist das ULD die Bürger vor dem Hintergrund, dass das ULD keine Betretungsrechte hinsichtlich privater Wohnungen und Grundstücke hat, in der Regel auf den Privatrechtsweg. Das Bundesdatenschutzgesetz ist bei der Datenverarbeitung zu persönlichen bzw. familiären Zwecken nicht anwendbar. Die Schlichtung privater Streitigkeiten ist nicht Aufgabe der Datenschutzaufsichtsbehörden.

Was ist zu tun?
Für die Beilegung von Nachbarschaftsstreitigkeiten sind grundsätzlich die Gerichte zuständig. Soweit keine öffentlichen Belange berührt sind, müssen die Beteiligten daher den Privatrechtsweg einschlagen.

5.8.8 Webcams schießen wie Pilze aus dem Boden

Immer häufiger erreichen das ULD Beschwerden von aufmerksamen Bürgern über Webcams, mit deren Hilfe Bilder von Landschaften oder von öffentlichen Plätzen im Internet dargestellt werden.

Das ULD prüft regelmäßig im Internet abrufbare **Webcambilder**, ob mit der Veröffentlichung der Aufnahmen gegen geltendes Datenschutzrecht verstoßen wird. Im Ergebnis war der Betrieb der überprüften Webcams zumeist – manchmal nach Veränderung der Einstellungen – zulässig.

Vor dem Hintergrund der Diskussion um eine Webcam in einem **schleswig-holsteinischen Ostseebad** hat das ULD seine Rechtsauffassung zum Einsatz von Webcams ausführlich dargelegt und veröffentlicht. Im konkreten Fall war das ULD insbesondere von den Zoommöglichkeiten auf einen bestimmten Strandabschnitt nicht unbedingt begeistert. Die Identifizierbarkeit von Menschen war aber so eingeschränkt, dass die Bilder akzeptiert werden konnten.



Beim Betrieb von Webcams müssen auch die Anforderungen des **Kunsturhebergesetzes** (KUG) erfüllt sein. Danach dürfen Bildnisse, auf denen die Personen nur als Beiwerk neben einer Landschaft oder einer sonstigen Örtlichkeit erscheinen, auch ohne Einwilligung der Betroffenen veröffentlicht werden, es sei denn, schutzwürdige Interessen der Abgebildeten stehen einer Veröffentlichung entgegen. Zeigen Webcams Orts- oder Landschaftsaufnahmen und lassen sich einzelne Personen nur mit besonderem Zusatzwissen identifizieren, so besteht für das ULD kein Anlass zum Eingreifen.

Durch vorhandene **Zoomfunktionen bzw. Vergrößerungsmöglichkeiten** der einzelnen Bilder können durchaus schutzwürdige Interessen von Betroffenen einer Veröffentlichung entgegenstehen, wenn etwa hochauflösende Bilder dargestellt und bestimmte räumliche Bereiche, wie z. B. Kindergärten, Spielplätze, Toilettenanlagen, Eingänge zu Justizvollzugsanstalten, von der Webcam erfasst werden. Derartiges fanden wir aber in Bezug auf Webcams in Schleswig-Holstein nicht vor.

Was ist zu tun?
Die weitere Entwicklung von Webcams muss kritisch beobachtet werden, damit eingeschritten wird, wenn die schutzwürdigen Interessen der Betroffenen gegenüber den Veröffentlichungsinteressen überwiegen.

5.8.9 Unbeachtete Werbewidersprüche

Ein ehemaliger Bankkunde erhielt wiederholt Werbung seiner früheren Bank, obwohl er der Nutzung seiner Daten für Werbezwecke widersprochen hatte. Wir mussten ein Bußgeld verhängen.

Nach dem BDSG hat jeder Betroffene das Recht, gegenüber der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder Markt- und Meinungsforschung zu widersprechen. Der Widerspruch macht die Datennutzung für diese Zwecke unzulässig, so auch im geschilderten Fall. Die Reaktion der verantwortlichen Bank gab uns Grund zur Sorge, denn sie ließ schwerwiegende Mängel der innerbetrieblichen Organisation erkennen. Es war technisch und organisatorisch nicht gewährleistet, dass der Widerspruch **mit Werbedaten vollständig abgeglichen** wurde bzw. werden konnte. Dies führte dazu, dass der Widerspruch des Betroffenen nicht beachtet wurde. Der Bußgeldbescheid ist rechtskräftig.

Was ist zu tun?
Gemäß dem BDSG muss eine Stelle sicherstellen, dass Widersprüche beachtet werden. Sie muss gewährleisten, dass bei der Datensperrung Datensatzabweichungen erkannt und berücksichtigt werden.

5.8.10 Behinderung der Aufsichtstätigkeit des ULD

Das ULD ist zur Erfüllung seiner Aufgaben auf die Mitwirkung der verantwortlichen Stellen angewiesen. Diese müssen Prüfungshandlungen in ihren Geschäftsräumen dulden und dem ULD die für dessen Tätigkeit erforderlichen Auskünfte erteilen. In der Praxis wird dies nicht immer beachtet.

Für Datenschutzermittlungen hat das ULD das Recht, Geschäftsräume von verantwortlichen Stellen zu betreten und **vor Ort Prüfungen vorzunehmen** (32. TB, Tz. 5.3.2).

Nicht weniger wichtig für die Aufgabenerfüllung des ULD ist dessen Auskunftsrecht. Verantwortliche Stellen müssen uns die für die Erfüllung unserer gesetzlichen Aufgaben erforderlichen Auskünfte erteilen, auch auf schriftliche Anfragen. Eine Ausnahme gilt, wenn sich der Auskunftspflichtige durch die Beantwortung der Fragen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Das ULD weist in seinen Auskunftsersuchen stets auf die **Auskunftspflicht** und auf das Recht zur Verweigerung der Auskunft hin. Soll vom Auskunftsverweigerungsrecht Gebrauch gemacht werden, ist dies dem ULD mitzuteilen.



Dessen ungeachtet unterlassen verantwortliche Stellen Rückmeldungen, nicht selten sind die Auskünfte lückenhaft. Oft bedarf es mehrfachen und nachdrücklichen Nachfragens, die verantwortliche Stelle dazu zu bringen, den Sachverhalt umfassend aufzuklären und uns eine vollständige und richtige Auskunft zu erteilen. Die Nichterteilung sowie die nicht richtige, nicht vollständige und nicht rechtzeitige Erteilung der Auskunft stellen eine **Ordnungswidrigkeit** dar, wenn die verantwortliche Stelle sich nicht auf ein ihr zustehendes Auskunftsverweigerungsrecht beruft. In Fällen, in denen die Auskunft uns gegenüber nicht oder nicht vollständig, richtig oder rechtzeitig erteilt wurde, werden vom ULD in der Regel Bußgeldverfahren eingeleitet. Das Amtsgericht Kiel bestätigte die Bußgeldbescheide, sofern dagegen Einspruch eingelegt wurde, dem Grunde nach.

6 Systemdatenschutz

6.1 Erforderlichkeit und Angemessenheit

Das LDSG fordert, dass bei der Verarbeitung personenbezogener Daten die erforderlichen und angemessenen Sicherheitsmaßnahmen getroffen werden müssen. Das ULD hat in vielen Projekten bei der Risikoanalyse, Beurteilung und Maßnahmenauswahl eine beratende Funktion.

Viele Daten verarbeitende Stellen haben Probleme, die Erforderlichkeit von **technischen und organisatorischen Maßnahmen** nachvollziehbar herzuleiten und die Angemessenheit der getroffenen Maßnahmen zu beurteilen. Kaum ein Satz des Landesdatenschutzgesetzes (LDSG) formt die Datenverarbeitung so stark wie die Regelung zur Datensicherheit. Darin sind Anforderungen an die Datenverarbeitung gestellt, die sich in den aktuellen Sicherheitsstandards – wie der ISO 27000er-Normenwelt oder der Grundschutz-Vorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – wiederfinden.

Erster Grundsatz ist die Erforderlichkeit. Technische und organisatorische Maßnahmen müssen einem konkret ausgewiesenen Risiko entgegenwirken. Daten verarbeitende Stellen müssen darlegen, warum eine konkrete Sicherheitsmaßnahme getroffen wurde, und nachweisen, dass eine nachvollziehbare und belastbare Analyse der Risiken stattgefunden hat. Mit der Erforderlichkeitsprüfung legen IT-Planer dar, dass sie **Datenschutz, Datensicherheit und Wirtschaftlichkeit** in Einklang gebracht haben: Es werden nur Sicherheitsmaßnahmen für konkret benennbare Risiken getroffen, und es werden alle konkreten Risiken mit Sicherheitsmaßnahmen bedacht.

Im Wortlaut: § 5 Abs. 2 LDSG

Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen durch die Leiterin oder den Leiter der Daten verarbeitenden Stelle oder eine befugte Person freizugeben.

In der Praxis kommt diese entscheidende Planungsphase oft zu kurz. Häufig macht die Projektleitung den Fehler, eine Analyse der Risiken und eine Maßnahmenauswahl zu spät im Projekt durchzuführen. In vielen Fällen führt erst die drohende Vorabkontrolle durch behördliche Datenschutzbeauftragte oder durch das ULD dazu, dass die Projektleitung sich um die notwendigen Nachweise gemäß LDSG und Datenschutzverordnung (DSVO) kümmert. Unnötige finanzielle und personelle Aufwände entstehen so im Projekt. Diese „nacheilenden“ Risikoanalysen führen in der Regel zu deutlichem Nachbesserungsbedarf und so zu unerwünschten Projektverzögerungen oder -verteuerungen. **Die Risikoanalyse gehört an den Anfang eines Projekts**. Nur hier können frühzeitig die notwendigen Maßnahmen identifiziert werden.



In den Projekten finden sich häufig zwei unterschiedliche Ansätze zur Risikoanalyse. Der erste Ansatz fordert von allen Projektmitarbeitern und den Auftraggebern eine Analyse. Häufig wird in einer oder mehreren Sitzungen eine gemeinsame Risikosicht erarbeitet: Welche Risiken bestehen für die Datenverarbeitung? Welche Risiken sind tragbar, gegen welche Risiken muss etwas getan werden? Dieses Vorgehen betont sehr stark den Aspekt der **Erforderlichkeit**. Nur für identifizierte Risiken werden Maßnahmen getroffen. Dies führt in der Regel zu schlanken und wirtschaftlichen Sicherheitskonzepten. Es kann aber auch dazu führen, dass in der Analyse wesentliche Risiken nicht als solche identifiziert wurden. Die internationalen Standards der ISO 27000er-Reihe orientieren sich beispielsweise an diesem Ansatz.

Der zweite Ansatz zur Risikoanalyse orientiert sich am Vorgehen anderer vergleichbarer Organisationen. Arbeitet man in ähnlichen Ausgangssituationen mit ähnlichen Geräten und Programmen, so sind wahrscheinlich die Risiken und die zu treffenden Maßnahmen auch ähnlich. Der aufwendige Prozess der Risikoanalyse vorab kann abgekürzt werden. Man macht einfach das, was alle anderen in derselben Situation auch machen. Diese Vorgehensweise betont die **Wirksamkeit**. Die Wahrscheinlichkeit, dass bei diesem Ansatz wesentliche Risiken übersehen werden, ist deutlich geringer. Gleichzeitig steigt jedoch die Wahrscheinlichkeit, dass man aufgrund einer fehlenden spezifischen Analyse auch unangemessene Maßnahmen umsetzt und deutliche personelle und finanzielle Mehraufwände in Kauf nimmt. Bei besonders schutzbedürftigen Daten oder in ungewöhnlichen Einsatzszenarien ist eine zusätzliche spezialisierte Risikoanalyse notwendig. Dieses Vorgehen findet man in seinen Grundzügen in der Grundschutz-Vorgehensweise des BSI wieder.

Weiterer Prüfungspunkt ist die **Angemessenheit**. Für jede technische und organisatorische Maßnahme muss die Wirksamkeit überprüft und nachgewiesen werden. In unseren Beratungsprojekten stehen wir gemeinsam mit den Daten verarbeitenden Stellen immer wieder vor Sachverhalten, zu denen es bei Kontrollen heißt: „Eigentlich soll das aber funktionieren!“

Nur durch regelmäßige und anlassbezogene **Kontrollen** der Datenverarbeitung durch Datenschutz- und Sicherheitsbeauftragte kann festgestellt werden, ob die gewählten technischen und organisatorischen Maßnahmen wirken. Auch hierbei muss das Ziel einer Sicherheitsmaßnahme im Blick sein. Nur wenn die Sollvorgabe benannt ist, kann die Zielerreichung geprüft werden. Erfolgreiche Organisationen arbeiten nach dem Prinzip: „Für jede Maßnahme muss es eine messbare Kennzahl geben.“ Dieser an Kennzahlen orientierte Ansatz ist für Sicherheitsmaßnahmen nützlich und führt zu einer deutlichen Vereinfachung der Kontrollen.

Die Kontrollen werden automatisierbar. Durch die automatisierte Prüfung der Wirksamkeit vor allem von technischen Maßnahmen werden Datenschutz- und Sicherheitsbeauftragte von Routinetätigkeiten entlastet.

Was ist zu tun?
Das LDSG gibt mit den Grundsätzen der Erforderlichkeit und Angemessenheit die wirtschaftliche Umsetzung einer datenschutzkonformen Datenverarbeitung vor. IT-Projekte müssen diesen Maßgaben folgen. Es muss dafür gesorgt werden, dass eine Risikoanalyse und Maßnahmenauswahl frühzeitig im Projektverlauf stattfinden.

6.2 Der allmächtige anonyme Administrator

IT-Systeme bringen in aller Regel im Auslieferungszustand ein administratives Standardbenutzerkonto mit, das mit umfassenden Berechtigungen ausgestattet ist. Diese Annehmlichkeiten wissen nicht nur ehrliche Administratoren zu schätzen, sondern auch diverse externe und interne Angreifer.

Mal heißt dieses Benutzerkonto „Administrator“, mal „root“, mal „admin“, mal so wie der Systemhersteller. Es verfügt oft über alle Berechtigungen im System, was für den Administrator das Arbeiten mit diesem Konto nicht nur bei der Erstkonfiguration sehr angenehm gestaltet. Doch Vorsicht: **Schadprogramme** nehmen die Allmacht und Anonymität des administrativen Standardbenutzers ebenso gern in Anspruch wie manipulative Benutzer oder Cracker.

Für eine ordnungsgemäße Datenverarbeitung nach aktuellem Stand der Technik ist es zwingend notwendig, dass die administrativen Tätigkeiten nachvollziehbar sind. Das LDSG und die DSVO stellen hierfür konkrete Anforderungen. Bei jeder administrativen Tätigkeit muss stets der **Ausführende** ermittelt werden können.

Kommt es zu Fehlern, Störungen oder Sicherheitsproblemen in der Datenverarbeitung, muss verlässlich nachprüfbar sein, wer oder was die Fehler oder Störungen verursacht oder ermöglicht hat. Dementsprechend ist das Arbeiten mit personalisierten Administrationskonten zum Schutz der personenbezogenen Daten und gleichzeitig auch der Administratoren zwingend erforderlich.

> ***Im Wortlaut: § 6 Abs. 2 LDSG***
>
> *Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.*

Das ULD fordert, dass im Tagesgeschäft mit **personalisierten Benutzerkonten ohne administrative Rechte** gearbeitet wird. Die administrativen Rechte sollen nur anlassbezogen und gezielt erteilt werden. Wir empfehlen personalisierte und aufgabenbezogene Administrationskonten, deren Rechteprofil restriktiv zusammengesetzt ist.

Sprechen gewichtige Gründe gegen die Nutzung personalisierter Administrationskonten, so ist die Verwendung eines anonymen Administrationskontos nur akzep-

tabel, wenn andere Maßnahmen die Zuordnung zu einer Person ermöglichen. Als Beispiel können sich Administratoren häufig **fallweise administrative Rechte** über Befehle wie „sudo“ bei Unix-Systemen oder „Ausführen als …“ bei Windows-Systemen verschaffen. Die Nutzung dieser Funktionen muss nachvollziehbar dokumentiert werden.



Das Anlegen eines lokalen anonymen Administrationskontos muss dadurch gerechtfertigt sein, dass Systeme im Notfall administrierbar sein müssen. Die Gründe und das Vorgehen zur Dokumentation sind in solchen Fällen jeweils **schriftlich** im Administrations- bzw. Sicherheitskonzept sowie in der Systemakte darzulegen.

Die Vorgaben für die Verwendung eines **anonymen Administrationskontos** sind:

- eine hinreichende Protokollierung und Kontrolle,
- kein direktes Log-in mit dem anonymen Administrationskonto,
- regelmäßiger Wechsel des Passwortes des anonymen Administrationskontos,
- das Verwenden eines komplexen und langen (mehr als 12stelligen) Passwortes sowie
- die restriktive Vergabe der „sudo“- bzw. „Ausführen als …“-Berechtigung.

Über eine Protokollierung muss feststellbar sein, wer zu welchem Zeitpunkt das anonyme Administrationskonto genutzt hat und welche Programme bzw. Tätigkeiten ausgeführt wurden. Nur unter dieser Maßgabe ist von einer **pseudonymisierten Wahrnehmung der administrativen Rechte** auszugehen, da die administrativen Tätigkeiten im Nachgang dem personalisierten Benutzerkonto des Administrators zugeordnet werden können. Grundsätzlich darf nach der Grundkonfiguration eines Systems das direkte Anmelden mit einem anonymen Standardadministrationskonto nicht mehr möglich sein. Dies ist durch das Löschen oder das Deaktivieren der anonymen Standardkonten möglich oder indem diesen Konten die administrativen Berechtigungen entzogen werden.

Was ist zu tun?
Anonyme Administration ist nicht mit den Vorgaben des LDSG vereinbar. Ist die Nutzung personalisierter Administrationskonten in Einzelfällen nicht möglich, so sind durch automatisierte Protokollierung und regelmäßige Auswertung zusätzlich technische und organisatorische Maßnahmen zu treffen.

6.3 AAL − altersgerechte Assistenzsysteme

„Ambient Assisted Living“ soll Menschen im alltäglichen Leben eine situationsabhängige und unaufdringliche Unterstützung ermöglichen, wobei über Sensoren Personendaten automatisiert erfasst und ausgewertet werden, die oft zum besonders geschützten privaten Kernbereich des Menschen zählen.

Die Ausgestaltung des AAL hängt vom Unterstützungsbedarf der jeweiligen Nutzergruppe ab. Bei jüngeren, gesunden Menschen stehen Unterhaltung und Lifestyle-Funktionen zur Steigerung der Lebensqualität im Vordergrund. Bei alten und insbesondere hilfebedürftigen Menschen geht es darum, diesen ein **sicheres, selbstständiges Leben** im häuslichen Umfeld zu ermöglichen bzw. die Möglichkeit einer häuslichen Pflege zu verlängern.

Das ULD hat auf Initiative des Bundesministeriums für Bildung und Forschung (BMBF) eine Vorstudie zu den „Juristischen Fragen im Bereich altersgerechter Assistenzsysteme“ erstellt, deren Ziel es ist, im Kontext von 18 anwendungsorientierten Verbundprojekten die Technologie- und Anwendungsentwicklung beim AAL zu unterstützen. Neben dem Entwickeln wünschenswerter Lösungen sollten unerwünschte Wirkungen, etwa im Bereich des Datenschutzes, frühzeitig erkannt und vermieden werden.


https://www.datenschutzzentrum.de/aal/

In den technisch orientierten Partnerprojekten wurden Techniken für altersgerecht ausgestaltete Serviceleistungen entwickelt. Typische Teile dieser Serviceleistungen im Rahmen von AAL-Systemen zum Einsatz in Wohnungen oder Zimmern von Pflegeeinrichtungen sind Bewegungssensoren, Sturzmelder, Füllstandmelder (z. B. Aquastop-Systeme), die Überwachung von Vitaldaten zu Atmung, Puls, Körpertemperatur, Blutdruck, Gewicht, Blutzucker, telemedizinische Dienste, Abschaltsysteme etwa für Herd oder Licht, elektronisches Schließen und Öffnen von Fenstern und Türen, Notrufsysteme in Koppelung mit Dienstleistungen, Telefone oder Videoüberwachung in jedem Raum.

In einem geförderten Projekt wurde eine Plattform entwickelt, über die AAL-gestützte Betreuungsdienstleistungen zusammengestellt und beauftragt werden können. In einem anderen Projekt wurden Sensoren konzipiert, die anhand der Nutzung von Licht, Strom, Gas und Wasser, der Dusche und des Fernsehens schleichende Veränderungen des Gesundheitszustands und Notfälle, z. B. Stürze, erfassen sollen. Ein System erfasst mit u. a. im Bett installierten Sensoren kontinuierlich den Gesundheitszustand der Betroffenen. Die jeweils erzeugten Daten werden von einem Rechnersystem zusammengefasst und interpretiert. Über das Internet werden aktuelle Lageberichte dann an einen Notruf und an ein Sicherheitssystem weitergeleitet, das Angehörige, Pflegedienste, Hausärzte und Kliniken einbezieht. In einem weiteren Projekt werden Techniken zur Überwachung sportlicher Betätigungen von Personen entwickelt. Die wesentliche Funktion all dieser AAL-Systeme besteht darin, ein „Normalitätsprofil“ für eine Person zu entwickeln, um daran gemessen Unregelmäßigkeiten festzustellen und adäquat zu reagieren. In Notfällen sollen Tonwarnungen für den Betroffenen ausgegeben

oder eine Nachbarin, ein Verwandter oder ein professioneller Warndienst informiert werden. Diese können dann bei der Person anrufen, eine Videoverbindung aufbauen, eine Hilfsperson vor Ort beauftragen nachzuschauen oder einen Krankenwagen anfordern.

AAL-Systeme dienen, so das Konzept der meisten Projekte, der kostengünstigen Betreuung von hilfebedürftigen Menschen. Häufig sollen die Möglichkeiten einer häuslichen Pflege technisch verlängert werden, was zumeist im Interesse sowohl der meisten Pflegebedürftigen als auch der Kostenträger liegt. AAL-Systeme können die Autonomie körperlich eingeschränkter Menschen länger als bislang aufrechterhalten. Die Menschen sollen wählen können, wo sie sich aufhalten bzw. wohin sie sich begeben wollen. Dies ist ein wesentlicher Aspekt **individueller Selbstbestimmung**. Durch Nutzung von Technik soll die informationelle, körperliche und soziale Autonomie von Menschen länger erhalten bleiben.

Dies erfolgt zu dem Preis, dass sie einer technisierten Kontrolle ihrer körperlichen Verfassung und ihres Verhaltens unterworfen werden. Selbstbestimmung ist aber nur dann wirklich gewährleistet, wenn die Betroffenen mitbestimmen können, wie die Informationsverarbeitung der AAL-Dienstleister stattfindet. Der Konflikt zwischen zunehmender Freiheit und zugleich zunehmender Abhängigkeit durch Technik ist typisch für die arbeitsteilige Informationsgesellschaft. Er kann nur aufgelöst werden, wenn die Organisationen, die ihre Dienstleistungen der Pflege, der medizinischen Versorgung, der Beobachtung oder der Leistungsdokumentation technikunterstützt erbringen, ihre oft komplizierten technischen Systeme selbst beherrschen und sich zugleich einer externen Kontrolle unterwerfen. Die **Abhängigkeit von der Technik** darf nicht zu einer Abhängigkeit von den die Technik einsetzenden Organisationen führen, die eine hohe Gestaltungsmacht über den Alltag von Menschen innehaben.

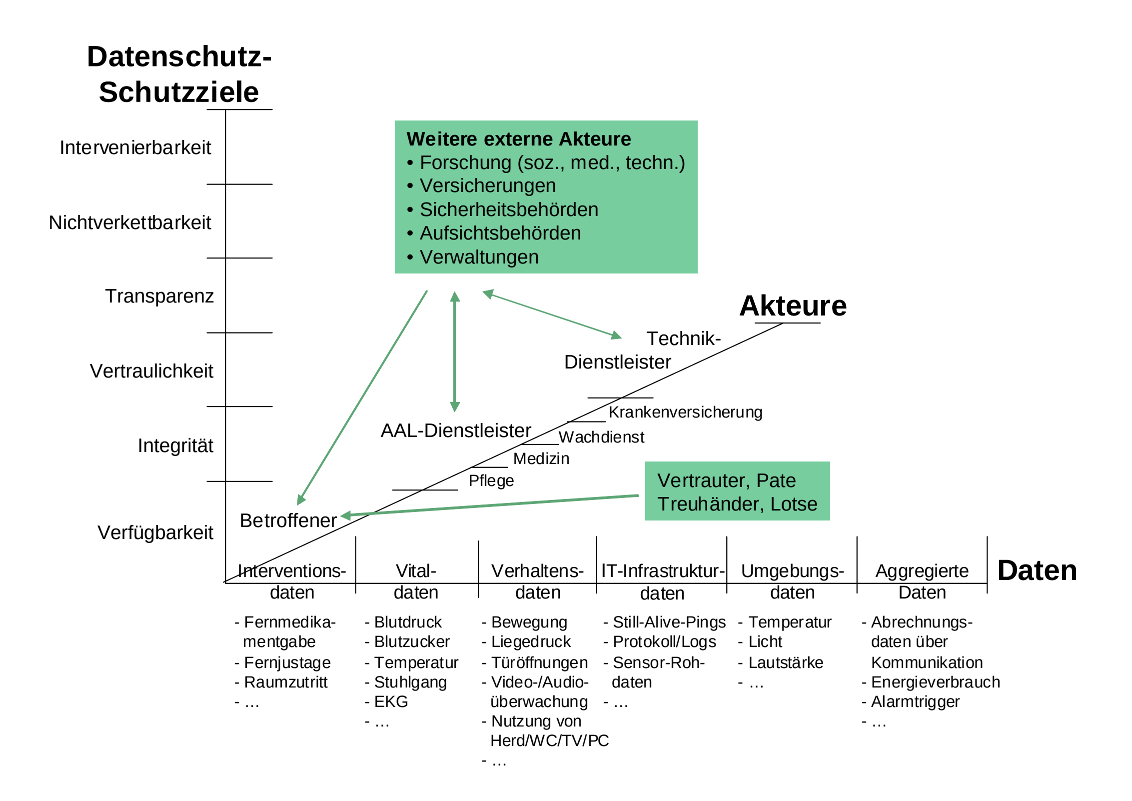
Haben Menschen mit der Veralltäglichung von AAL tatsächlich die Wahl, die Techniken selbstbestimmt und würdig zu nutzen? Wird es möglich sein, nach einer Zeit der Nutzung von AAL-Techniken der weiteren Nutzung zu widersprechen? Wird am Ende der voll vermessene Mensch stehen, dessen privaten Eigenschaften und Handlungen erforscht und zu einem Profil des Normalmenschen zusammengestellt sind? Tatsächlich besteht die Tendenz, Abweichungen von diesem **Normalprofil** zu erfassen. Werden die Betroffenen gegenüber ihren Versicherungen Rechenschaft für ihr Verhalten ablegen müssen? Freiheit und Selbstbestimmung bedeutet, dass man nicht dem standardisierten Normalmaß entsprechen und sich für Abweichungen rechtfertigen muss.

Die Studie zeigt die Grenzen eines Datenschutzes auf, der sich stark auf die **freiwillige und informierte Einwilligung** der Betroffenen stützt. Die Herausforderung liegt darin, den Anforderungen des Datenschutzes nicht über das Erteilen von Unmengen an rein formell bleibender Einwilligungen formal zu genügen, sondern materiell wirksam operativ zu sichern. Einwilligungen, so das Datenschutzrecht, müssen inhaltlich klar, freiwillig und informiert erfolgen. Doch gerade die von den Entwicklern der AAL-Systeme vorgesehene Klientel verfügt typischerweise über kein Wissen von komplexen informationstechnischen Systemen. Es ist deshalb eine wichtige Aufgabe beim Aufbau von AAL-Infrastruk-

turen, ein betroffenengerechtes Niveau an Transparenz und Wahlmöglichkeit herzustellen.

Ein Teil der Lösung des Problems besteht darin, Datenschutz in die Systeme von Anfang an einzubauen. Die AAL-Systeme müssen so funktionieren, dass sie, dem Paradigma der **Privacy-Enhancing Technologies** (PET) folgend, den grundrechtlich garantierten Datenschutz der Menschen unterstützen. Zudem sind die Hersteller und Betreiber der Systeme aufgefordert, Transparenz in hochauflösender professioneller Qualität insbesondere für Prüfinstanzen bereitzustellen.

In der Vorstudie wurde ein Modell entwickelt, mit dem die Datenschutzproblematik des AAL übersichtlich erfasst werden kann. In einer Matrix mit drei Dimensionen werden Daten, Akteure sowie – in die Form von Schutzzielen des Datenschutzes gebracht – die technischen und organisatorischen Anforderungen an die Verarbeitung der Daten bzw. Systeme durch die Akteure bzw. Prozesse erfasst.



Schon beim Ausfüllen dieser Matrix wird klar, welche **gesellschaftliche Gestaltungsaufgabe** vor Datenschützern, aber auch vor den Anbietern und Nutzern von AAL-Systemen liegt. Hersteller und Betreiber von AAL-Anwendungen müssen immer wieder daran erinnert werden, dass die „Unantastbarkeit der Würde des Menschen" mehr als eine ethische Forderung ist und gesetzlich zwingende praktische Konsequenzen hat.

Was ist zu tun?
In allen AAL-Projekten ist darauf hinzuwirken, dass die verschiedenen Akteure die Systeme so konstruieren, implementieren, konfigurieren und betreiben, dass diese den von den Schutzzielen formulierten Anforderungen genügen.

6.4 Tests und Fehlerbehebung mit Echtdaten

Die steigende Komplexität vernetzter Rechnersysteme führt zu komplexeren Fehlerszenarien. In Einzelfällen können Fehler laut Aussagen der Hersteller nur mit Echtdaten nachvollzogen werden. Der Schutz der personenbezogenen Daten muss hierbei sichergestellt bleiben.

Mit der Vielschichtigkeit der eingesetzten Software in Unternehmen und Verwaltungen steigt auch die Komplexität und Vielzahl der möglichen Fehlerbilder. Oft sind es nicht mehr die offensichtlichen, sondern **individuelle und schwer nachzustellende Fehler**, die Anwender und Hersteller beschäftigen. Solche Fehler sind besonders schwer zu vermitteln – sowohl nach innen als auch nach außen.

> ***Im Wortlaut: § 17 Abs. 1-3 LDSG***
>
> *Verarbeitung personenbezogener Daten im Auftrag, Wartung*
>
> *(1) Lässt eine Daten verarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Rechte der Betroffenen sind ihr gegenüber geltend zu machen. …*
>
> *(2) Die Daten verarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. … Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.*
>
> *(3) Sofern die Vorschriften dieses Gesetzes auf Auftragnehmende keine Anwendung finden, hat die Daten verarbeitende Stelle diese zu verpflichten, jederzeit von ihr veranlasste Kontrollen zu ermöglichen.*

Muss die Nutzung der Software bis auf Weiteres komplett eingestellt werden oder nur für ganz bestimmte Aktionen? War es ein Bedienungsfehler oder ist die Software fehlerhaft? Welche Tätigkeiten sind genau zum Zeitpunkt des Fehlers, davor und danach durchgeführt worden und von wem? Diese Analysen erfordern von der Daten verarbeitenden Stelle wie vom Softwarehersteller ein **hohes Maß an exakter Dokumentation**, effizienter Kommunikation und Kenntnis der Software. Trotz solcher Bemühungen ist es nicht immer gegeben, dass der Fehler zügig gefunden und behoben werden kann. In der Praxis können äußerst individuelle Sachverhalte auftreten. Hierfür existiert nicht immer ein passender Testdatensatz beim Hersteller. Der Fehler kann dann kaum mit vertretbarem Aufwand nachgestellt werden. Als Ausweg wird dann häufig die Übermittlung der Echtdaten an den Softwarehersteller geprüft, um die mitunter kostspielige Anreise eines Entwicklers zur Vorortanalyse zu vermeiden. Das ULD bearbeitet viele Anfragen zu diesem Themenbereich. Häufig handelt es sich um größere Projekte wie neue kommunale Kassenverfahren oder das Zusammenführen von Daten nach einer Verwaltungsfusion. Unter welchen Bedingungen ist eine solche Datenübermittlung und Datenverarbeitung beim Softwarehersteller zulässig?

Zunächst ist zu prüfen, ob eine **Auftragsdatenverarbeitung** – etwa im besonders sensiblen Bereich der Gesundheits- und Sozialdaten – überhaupt zulässig ist. Ist diese möglich, so sind explizite vertragliche Regelungen zu treffen, die die Anforderungen zur Auftragsdatenverarbeitung auf Systemen des Softwareherstellers oder zur Fernwartung auf organisationseigenen Systemen erfüllen. Das LDSG fordert konkrete schriftliche Vorgaben und Aufträge, insbesondere zu technischen und organisatorischen Sicherheitsmaßnahmen. Gemäß der DSVO muss die Daten verarbeitende Stelle – also der Auftraggeber – die beim Auftragnehmer getroffenen technischen und organisatorischen Sicherheitsmaßnahmen dokumentieren.

Wird die Fehleranalyse im Produktivsystem durchgeführt, so sind strikte Regelungen zur Fernwartung zu treffen. Das ULD forderte regelmäßig eine **Vollprotokollierung aller Tätigkeiten** der externen Dienstleister, verbunden mit einer regelmäßigen Auswertung unter Beteiligung des oder der behördlichen Datenschutzbeauftragten.

Wird die Fehleranalyse mit Echtdaten in einer vom Hersteller bereitgestellten Umgebung durchgeführt, so ist auf eine **strikte Trennung** der verwendeten Systeme zu Systemen anderer Kunden zu achten. Der Hersteller muss angemessene Sicherheitsmaßnahmen zur Kontrolle des Zugriffs, zur Durchsetzung der Datentrennung und zur Dokumentation der Sicherheitsmaßnahmen umsetzen.

Die Angemessenheit und Wirksamkeit dieser vertraglich vereinbarten Maßnahmen sind durch Kontrollen vorab, während und nach jeder Datenverarbeitung durch die verantwortliche Stelle zu überprüfen. Ist eine Software so anfällig und komplex, dass Fehler nur mit möglichst realistischen und großen Datenvolumen rekonstruiert werden können, empfiehlt sich dringend das Erstellen und Pflegen eines anonymisierten Testdatenbestandes auf Basis der Echtdaten beim Auftragnehmer.

Was ist zu tun?
Tests mit Echtdaten sind datenschutzrechtlich von hoher Relevanz. Auftraggeber und Auftragnehmer müssen spezielle Sicherheitsmaßnahmen treffen, um solche Tests im Einzelfall durchführen zu können. Dauerhafte Tests mit Echtdaten sind mit den Vorgaben des LDSG nicht vereinbar und werden vom ULD beanstandet.

6.5 Data Warehouses in der öffentlichen Verwaltung

Die Grundsätze der Zweckbindung und der Datensparsamkeit verbieten den Einsatz von Data Warehouses in der öffentlichen Verwaltung in aller Regel. In Ausnahmefällen sind sie jedoch datenschutzkonform möglich, wenn die Prozesse zur Datenauswertung unter dauerhafter Kontrolle des behördlichen Datenschutzbeauftragten stehen.

In Data Warehouses werden Daten **unterschiedlicher Quellsysteme zusammengeführt**. Kopien der Daten werden üblicherweise in einem separaten Datenbank-

system vorgehalten und dort ausgewertet. Data Warehouses dienen dann als Ausgangsbasis für das Data Mining, also für das „Schürfen“ von Informationen. Ziel ist es, bisher unerkannte Zusammenhänge in großen Datenmengen zu finden.

In der öffentlichen Verwaltung stoßen Data Warehouses mit personenbezogenen Daten an die **engen Grenzen der Zweckbindung**. Personenbezogene Daten, die zu einem bestimmten Zweck erhoben wurden, dürfen nicht der wahlfreien Auswertung zu anderen Zwecken zur Verfügung stehen.

Sollen personenbezogene Daten in einem Data Warehouse verarbeitet werden, so ist jede Auswertung vorab auf die Einhaltung der Zweckbindung zu prüfen. Eine wahlfreie Auswertung ist mit den Vorgaben des LDSG nicht vereinbar. Jede Auswertung muss vorher durch den oder die behördliche Datenschutzbeauftragte kontrolliert und durch die Leitung der Daten verarbeitenden Stelle freigegeben werden. Die **Kontrollen und Freigaben** sind zu dokumentieren.

Dies stellt hohe Anforderungen sowohl an die behördlichen Datenschutzbeauftragten als auch an die Dienststellenleitung. Bei der Einführung eines Data Warehouse ist deshalb bereits zu Beginn des Projektes auf eine intensive Vorbereitung, Unterrichtung und **Schulung der behördlichen Datenschutzbeauftragten** und der Leitung zu achten. Der Betrieb eines Data Warehouse ohne einen behördlichen Datenschutzbeauftragten mit spezieller Weiterbildung ist nicht datenschutzkonform.

Das ULD empfiehlt, zusätzlich die Rolle eines **Data Warehouse Controllers** einzuführen, der die notwendigen Kontroll- und Freigabeprozesse koordiniert und revisionssicher dokumentiert. Jede Anforderung einer Auswertung muss durch den Data Warehouse Controller in einen konkreten Auftrag überführt werden. Der Auftrag zur Auswertung muss geprüft und freigegeben werden. Liegen die Ergebnisse der Auswertung vor, so sind diese wiederum zumindest auf die Vereinbarkeit mit den datenschutzrechtlichen Vorgaben zu prüfen, bevor sie an die anfordernde Organisationseinheit weitergegeben werden. Nur durch enge Einbeziehung der behördlichen Datenschutzbeauftragten und stetige Befassung der Leitung der Daten verarbeitenden Stelle kann das Risiko des permanenten Rechtsverstoßes angemessen behandelt werden.

Noch stehen Data Warehouses in der **öffentlichen Verwaltung in Schleswig-Holstein** am Anfang ihrer Entwicklung. Das ULD erhält aber zunehmend Anfragen. In einem erfolgreichen Beratungsprojekt mit der Landespolizei (Tz. 4.2.2) wurden gemeinsam erste Grundsätze für den Einsatz eines Data Warehouse festgelegt.

Was ist zu tun?
Plant eine öffentliche Stelle ein Data Warehouse, so sind frühzeitig der behördliche Datenschutzbeauftragte und das ULD zu beteiligen, die darauf achten müssen, dass jederzeit und ausnahmslos die Vorgaben zur Datentrennung, Datensparsamkeit und Zweckbindung beim Data Mining umgesetzt werden.

6.6 Ergebnisse aus Überprüfungen und Kontrollen vor Ort

6.6.1 Kooperative Regionalleitstelle Nord in Harrislee

Das ULD prüfte in Zusammenarbeit mit dem Innenministerium die Kooperative Regionalleitstelle in Harrislee und stellte teilweise erhebliche Mängel fest. Deren Behebung wird vom Innenministerium begleitet.

Es ist eher ungewöhnlich, dass eine Daten verarbeitende Stelle um eine datenschutzrechtliche und sicherheitstechnische Prüfung bittet. Das Innenministerium ist diesen ungewöhnlichen Weg gegangen, um eine zusätzliche Kontrolle der sicherheitstechnischen Absicherung und der Datenschutzaspekte in der Leitstelle durchzuführen. Die Kooperative Regionalleitstelle (KLRS) Nord ist eine **gemeinsame Einrichtung** der Landespolizei und der Kreise Nordfriesland und Schleswig-Flensburg sowie der Stadt Flensburg. Darin wurden die polizeilichen und nicht polizeilichen Leitstellen zusammengefasst. Polizeiliche und nicht polizeiliche Aufgaben werden bei gemeinsamer Nutzung der baulichen und technischen Einrichtungen organisatorisch getrennt wahrgenommen. Beide Bereiche werden jeweils eigenständig von einem Leiter geführt.

Die in der Prüfung erkannten Mängel wurden bereits während der Prüfungen vor Ort bewertet, mögliche Maßnahmen zur Mängelbehebung wurden besprochen und in einigen Fällen wurde die Behebung sofort gestartet. Andere Mängel mussten mit den Herstellern der Leitstellensysteme, der Betriebsmannschaft vor Ort und im Landespolizeiamt im Nachgang bewertet und in einen Plan zur Mängelbehebung aufgenommen werden. Die Prüfung zeigte, dass eine unabhängige Kontrolle bei Großprojekten wie der Kooperativen Leitstelle ein wichtiger Baustein der Qualitätssicherung sein kann. Die Kontrollergebnisse von Harrislee werden in die vereinbarten Prüfungen der übrigen Kooperativen Leitstellen in Schleswig-Holstein einfließen.

Was ist zu tun?
Die Kooperative Leitstelle muss die durch das ULD aufgezeigten sicherheitstechnischen Mängel beheben. Das Innenministerium muss sicherstellen, dass die gewählten Maßnahmen zur Mängelbehebung auch in den anderen Kooperativen Regionalleitstellen wirksam werden.

6.6.2 Prüfung beim Wasser- und Bodenverband Ostholstein

Eine Software, die das „private Surfen im Internet“ verhindern soll, bietet gleichzeitig die Möglichkeit, automatisch zu protokollieren, welche Programme wie lang auf den PCs von Mitarbeitern laufen.

Findet eine automatisierte **verdeckte Überwachung der Mitarbeiter-PCs** statt? In einer Petenteneingabe wurde eine auf den Arbeitsplatz-PCs beim Wasser- und Bodenverband Ostholstein installierte Software beschrieben, die auch eine Protokollierung der Tätigkeiten auf dem PC des jeweiligen Mitarbeiters aufzeichnet. Die Verwaltungsleitung hatte einen externen Dienstleister mit einer Lösung

beauftragt, die das „private Surfen im Internet“ der Mitarbeiter unterbindet. Der Dienstleister installierte eine Software, die weit mehr als das Sperren von Internetseiten ermöglichte. So konnte eine automatische Protokollierung aller Aktivitäten auf dem Arbeitsplatzrechner aktiviert werden. Bedingt durch Probleme mit einem Buchhaltungsprogramm wurde die Software wieder deinstalliert. Eine Durchsicht der Arbeitsplatz-PCs bestätigte dies. Um sich nicht dem Verdacht der unzulässigen automatisierten Leistungs- und Verhaltenskontrolle auszusetzen, will der Verband eine organisatorische Regelung schaffen, die die private Nutzung des Internets verbietet. Von der vorübergehenden Kontrolle erfasst wurden

- die installierte Programmliste,
- die Programmverzeichnisse im Windows Explorer,
- die Systemsteuerung und
- die Windows Registry.

Was ist zu tun?
Das Einhalten der Datenschutzvorgaben für den Wasser- und Bodenverband wird regelmäßig überprüft werden.

6.6.3 Prüfung im Amt Horst-Herzhorn

Eine gute Wahl!

Im Rahmen der Verwaltungsstrukturreform fusionierten Anfang 2008 die Ämter Herzhorn sowie Horst und erhielten den Namen „Amt Horst-Herzhorn“. Trotz der personellen und organisatorischen Problemstellungen wurde der Datenschutz nicht außer Acht gelassen. Die Leitungsebene zeigte mit der **Besetzung der Administratorenstelle** Weitblick und bewies, dass es sich lohnt, die Aufgaben der IT eine engagierte Mitarbeiterin durchführen zu lassen.

Unsere Überprüfung zeigte den **hohen Stellenwert des Datenschutzes** in dieser Verwaltung. Die in dem Datenschutzkonzept dokumentierten Sicherheitsmaßnahmen werden wirksam umgesetzt. Dank effektivem IT-Management und überdurchschnittlich guter Systemdokumentation wird auch bei Krankheit oder Urlaub der Administratorin die Verwaltung der IT-Umgebung durch andere explizit berechtigte Personen gewährleistet. Die durch das LDSG und DSVO geforderte Dokumentation hebt die Verwaltung deutlich vom Durchschnitt der im Land vorgefundenen Gegebenheiten ab. Es wurden keine Mängel festgestellt – ein seltener, erfreulicher Befund!

Was ist zu tun?
Die Amtsverwaltung sollte das gute Datenschutzniveau beibehalten.

6.6.4 Prüfung bei der KLG Heider Umland

Die datenschutzrechtliche Überprüfung der Kirchspielslandgemeinde Heider Umland führte zu einer äußerst hohen Anzahl von Beanstandungen.

Bei einer routinemäßigen Überprüfung des Amtes Kirchspielslandgemeinde Heider Umland fanden wir eine Vielfalt datenschutzrechtlicher Mängel vor. Folgende Punkte führten zur **Beanstandung**:

- Es wurde keine Stellvertretung für den Administrator ausgebildet.
- Der Administrator protokolliert seine administrativen Tätigkeiten nicht.
- Es erfolgt keine Kontrolle der Tätigkeiten des Administrators durch die Verwaltungsleitung.
- Es existieren keine vertraglichen Regelungen mit dem externen Dienstleister.
- Es wurde keine Verfahrensdokumentation erstellt.
- Ebenso fehlen die Dokumentationen der Sicherheitsmaßnahmen, der Tests und der Freigaben.
- Es wurden keine Arbeitsanweisungen (IT-Dienstanweisungen) für die Administration erstellt.
- Auf den zentralen Druckern, die auch für Unbefugte jederzeit erreichbar sind, wurden keine zusätzlichen Sicherheitsmaßnahmen getroffen.
- Auf den Notebooks war keine Verschlüsselungssoftware installiert.
- Die Aktenvernichtungscontainer waren nicht verschlossen und für Unbefugte leicht erreichbar.
- Die Archivräume wurden unverschlossen vorgefunden.

Was ist zu tun?
Die datenschutzrechtlichen Mängel sind umgehend zu beheben. Das ULD hat der Amtsverwaltung seine Beratung angeboten. Die Mängelbehebung wird von uns durch mehrere Nachkontrollen sichergestellt.

6.6.5 Nachprüfung bei der Stadtverwaltung Ratzeburg

Das ULD schließt Prüfungen erst ab, wenn alle erkannten Mängel nachvollziehbar behoben wurden. Die Mängelbehebung wurde in der Stadtverwaltung Ratzeburg durch eine Nachkontrolle begleitet.

In der Stadtverwaltung Ratzeburg erfolgte im November 2008 eine stichprobenartige Überprüfung der technischen und organisatorischen Sicherheitsmaßnahmen. Ihr Ziel war es, zusammen mit den Mitarbeitern in der automatisierten Datenverarbeitung eventuelle **Schwachstellen zu erkennen**. Die Erörterung der festgestellten Sachverhalte mit den Mitarbeitern und Verantwortlichen sollte dazu führen, dass sie die Notwendigkeit organisatorischer und technischer Sicherheits-

maßnahmen erkennen und diese zukünftig in die Organisation und Administration der automatisierten Datenverarbeitung einfließen lassen.

Die Stadtverwaltung erkannte im April 2009 unsere Beanstandungen sowie die **Vorschläge zur Behebung der Mängel** an. Verschiedene Maßnahmen seien schon umgesetzt. Die umfassende Darstellung aller Handlungen wurde für Mitte Mai angekündigt. Erst Ende Juli erhielten wir einen Bericht über die „Durchführung von Maßnahmen zur Beseitigung von Mängeln/Beanstandungen", in dem erläutert wurde, dass der Dokumentationspflicht gemäß LDSG und DSVO nachgekommen wurde, die notwendigen Regelungen jedoch aufgrund von personellen und organisatorischen Umstrukturierungsmaßnahmen noch nicht in Kraft gesetzt werden konnten. Dies sei für Ende September 2009 vorgesehen.

Die **Nachprüfung** sollte nun zeigen, ob die Mängelbehebung erfolgreich war. Wir stellten fest, dass immer noch nicht alle dokumentierten Regeln in Kraft gesetzt waren. Sie waren zwar mit Stand April 2009 aktualisiert, von der Verwaltungsleitung aber noch nicht unterschrieben. Der Bürgermeister gab dafür personelle und organisatorische Gründe an. Die endgültige Fertigstellung war für Ende 2010 vorgesehen. Das ULD wird die Umsetzung zeitnah abschließend prüfen. Wir hatten ferner festgestellt, dass eine Stellvertretung für den Administrator nicht mehr vorhanden war. Die Verwaltungsleitung berichtete uns von Überlegungen, administrative Aufgaben den Fachbereichen zu übertragen. Dies wurde bis zum Zeitpunkt der Prüfung jedoch nicht durchgeführt. Somit obliegt einer Person die Administration der hochkomplexen IT der Stadtverwaltung. Ein unzumutbarer Zustand, den das ULD mit Nachdruck beanstandete. Wir boten weiterhin unsere Beratung an.

Was ist zu tun?
Eine Stellvertretung für die Administration muss umgehend ausgebildet werden. Die Auslagerung administrativer Aufgaben in einzelne Fachabteilungen ist zügig umzusetzen. Das ULD wird weitere Nachkontrollen durchführen.

7 Neue Medien

Endlich hat die politische Diskussion über die Regulierung des Datenschutzes im Internet begonnen (Tz. 2.2). Die Notwendigkeit hierfür besteht schon seit einigen Jahren. Die aggressive Vorgehensweise von US-amerikanischen Firmen auf dem deutschen bzw. europäischen Markt – allen voran Facebook, dicht gefolgt von Google (Tz. 7.2) – macht offensichtlich, dass hier auf politischer wie auf administrativer Ebene schnell und grundsätzlich gehandelt werden muss, wenn die **Erosion der informationellen Selbstbestimmung** im weltweiten Netz gestoppt werden soll. Dabei spielt die Europäische Union mit ihren Regulierungsmöglichkeiten eine zunehmende Rolle (Tz. 11.1).

7.1 Eine neue – datenschutzkonforme – Rundfunkfinanzierung braucht das Land!

Die grundlegende Reform des Systems der Erhebung der Rundfunkgebühren sieht vor, die bisherige gerätebezogene Gebühr durch einen Beitrag für jede Wohnung bzw. Betriebsstätte zu ersetzen. Der Regelungsvorschlag ist gekennzeichnet durch die Schaffung umfassender Erhebungsbefugnisse und die Verletzung fundamentaler Prinzipien des Datenschutzrechts.



Ziel des Systemwechsels ist die Wahrung der Finanzsicherheit für die öffentlich-rechtlichen Rundfunkanstalten. Auslöser hierfür war nicht die Ausforschung der Gebührenpflichtigen, sondern dass Rundfunkgeräte von sonstigen IT-Geräten nicht mehr eindeutig unterschieden werden können und so jeder Computer die Gebührenpflicht auslöste. Das neue Beitragsmodell sollte auch eine höhere Beitragsgerechtigkeit und eine **datenschutzgerechtere Beitragserhebung** gewährleisten. Anknüpfungspunkt des neuen Beitrags wird die Wohnung bzw. die Betriebsstätte sein. Sämtliche Bewohnerinnen und Bewohner einer Wohnung werden als Gesamtschuldner für die Zahlung des Rundfunkbeitrags haften. Die Beitragsschuld tritt unabhängig davon ein, ob ein Gerät zum Empfang von Rundfunksendungen vorgehalten wird oder nicht.

Im Interesse des Schutzes der Privatsphäre kann die jahrelang umstrittene Kontrolle des Vorhaltens von Empfangsgeräten durch die Rundfunkgebührenbeauftragten und Gebühreneinzugszentrale (GEZ) entfallen. Die neue Beitragspflicht macht andere Datenarten aus anderen Quellen erforderlich. Die für den Beitragseinzug verantwortlichen Stellen benötigen nun ein Register der in Deutschland existierenden **Wohnungen und der darin lebenden Personen**. Denn nur einmal pro Wohneinheit soll der Beitrag entrichtet werden müssen. Zugleich soll sichergestellt werden, dass bei einem Auszug die Wohnung nicht aus der Beitragspflicht „entschwindet".

Die Datenschutzaufsichtsbehörden kritisierten die strenge Anknüpfung der Beitragspflicht an die Wohnung. Ein flächendeckender Beitragseinzug soll nur durch minutiöse Ausforschung der **in einer Wohnung lebenden Personen** realisierbar sein. Die bei den Meldebehörden bestehenden Melderegister geben keine Auskunft, welche Personen in einer Wohnung zusammenleben. Derartige Erfassungen sollen nunmehr erfolgen. Die Aufsichtsbehörden schlugen deshalb andere Anknüpfungspunkte vor, z. B. die Einkommenssteuerpflicht.

Mit dem Systemwechsel wird also die langjährig kritisierte Praxis der umfangreichen **Ausforschung durch die Rundfunkanstalten** nicht beendet, sondern nur modifiziert. Die bisherigen Datenerhebungstatbestände wurden leicht geändert und sogar ausgeweitet. Zusätzliche Rechtsgrundlagen für die Datenverarbeitung wurden geschaffen. Der Vorschlag ist durch übermäßige und unverhältnismäßige Datenverarbeitungsbefugnisse der Rundfunkanstalten und ihrer Hilfsorgane, durch fehlende Normklarheit und mangelnde Transparenz geprägt.

Der Entwurf missachtet grundlegende Datenschutzprinzipien. Er ermächtigt die Landesrundfunkanstalten zur Datenerhebung für die Beitragsfestlegung ohne Kenntnis der Betroffenen bei öffentlichen und nicht öffentlichen Quellen. Der **Grundsatz der Direkterhebung** von Daten wird dadurch entwertet. Eine Erfassung und Verarbeitung der Daten der Betroffenen erfolgt ohne ihre Kenntnis. Die Abweichung vom Prinzip der Direkterhebung ist im Entwurf nicht bestimmt und klar genug geregelt.

Wohl sollen sämtliche Beitragspflichtige einer **Meldepflicht** unterliegen. Sie sollen die im Staatsvertragsentwurf genannten Daten selbst anliefern. Ist für eine Wohnung kein Wohnungsinhaber bekannt, so stehen den Rundfunkanstalten fast unbeschränkte Möglichkeiten offen, die Nutzer der Wohnung oder Betriebsstelle zu ermitteln. Ungeregelt bleiben das Verhältnis zu den bereichsspezifischen Vorschriften der jeweiligen öffentlichen Quellen, z. B. in Meldegesetzen oder in der Grundbuchordnung, und die Art der zulässigerweise zu erhebenden Daten.

Der Zugriff auf nicht öffentliche Quellen und der Erhebungsumfang werden nicht hinreichend konkretisiert. Erklärter Wille ist es, über diese Ermächtigung weiterhin Daten von **privaten Adresshändlern** anzukaufen. Ein solcher Ankauf für Zwecke des Adressabgleichs ist nach Auffassung des ULD und anderer Aufsichtsbehörden weder erforderlich noch angemessen. Die Rundfunkanstalten haben bereits jetzt die Möglichkeit des Zugriffs auf geprüfte und qualitätsgesicherte Melderegisterdaten. Die Nutzung ungeprüfter Adresshändlerdaten begrün-

det eine große Gefahr der Nutzung fehlerhafter Daten. Dieser Ankauf ist eine Überprüfung ins Blaue hinein, also keine zielgerichtete Datenerhebung.

Es bedarf dringend der Klarstellung, dass Daten ausschließlich **beim Betroffenen zu erheben** sind und nur in begründeten Ausnahmefällen ein Rückgriff auf öffentliche Quellen zulässig ist. Die spezialgesetzlichen Erhebungs- und Verarbeitungsbefugnisse dürfen durch die Rechtfertigungstatbestände des Rundfunkbeitragsstaatsvertrages nicht umgangen werden. Die Grundsätze der Datensparsamkeit und Transparenz der Datenverarbeitung müssen durchgängig gewahrt werden.

Was ist zu tun?
Der Landtag Schleswig-Holstein sollte auf eine datenschutzkonforme Ausgestaltung des 15. Rundfunkänderungsstaatsvertrages drängen, um die nachhaltige Finanzierung des öffentlichen Rundfunks nicht mit dem Makel der unverhältnismäßigen Datenverarbeitung zu belasten.

7.2 Street View – visueller, 3-D- und Funk-Blick über den Gartenzaun

Die Hoffnung, Google hätte aus den Kontroversen des Jahres 2009 gelernt und würde den Datenschutz bei der Implementierung von Street View gesetzlich beachten, war trügerisch.

Das Thema Google Street View beschäftigt das ULD seit über zwei Jahren (32. TB, Tz. 7.2). Bereits im Jahr 2008 hatte sich der Landtag des Dienstes angenommen. Schleswig-Holstein diskutierte früh öffentlich und breit über die damit verbundenen persönlichkeitsrechtlichen Gefahren. Dies geschieht inzwischen bundes- und europaweit auf höchster Ebene. In enger Abstimmung mit dem ULD und den anderen Aufsichtsbehörden des Bundes und der Länder vertrat der Hamburgische Beauftragte für den Datenschutz die Interessen gegenüber der Google Germany GmbH als Vertreterin der Google Inc./USA. Ergebnis der Diskussion um die Zulässigkeit des Dienstes war ein **13-Punkte-Katalog**. Dazu gehört u. a. die Berücksichtigung der Widersprüche von betroffenen Bürgerinnen und Bürgern. Nur soweit die in dem Katalog enthaltenen Anforderungen erfüllt sind, ist der Einsatz des Dienstes datenschutzrechtlich nicht zu beanstanden.

? ***Google Street View***
Der von der Google Inc. betriebene Internetdienst Google Street View bildet Straßenpanoramen im Internet ab. Der Nutzer hat die Möglichkeit, virtuell aufgenommene Straßen zu „durchfahren“. Diese Bildaufnahmen wurden mittels Kameras erstellt, die auf Fahrzeugen in 2,90 m Höhe installiert waren.


http://www.datenschutzzentrum.de/geodaten/

Nach Angaben des Unternehmens hatte die Google Inc. bereits im Frühjahr 2010 90 % Deutschlands erfasst. Das **systematische Fotografieren der Straßenzüge** und die Veröffentlichung im Internet ist eine Erhebung und Verarbeitung perso-

nenbeziehbarer Daten, denn die von der Erfassung betroffenen Immobilien geben Auskunft über die Lebenssituation der dort Wohnenden. Die mit den Aufnahmen verknüpften Angaben zur Georeferenzierung können als Anknüpfungspunkt für weitere Informationen dienen und haben das Potenzial zur Profilbildung.

Im Zuge der Diskussionen um die Zulässigkeit der Erstellung und Veröffentlichung der Bildaufnahmen teilte die Google Inc. mit, nicht nur Fotos erstellt zu haben. Per **Laserscan** wurde ein dreidimensionales Abbild der fotografierten Häuser und der Umgebung erstellt. Mit dieser Vermessung sollen die Bilder in ein grafisches Modell eingebunden werden. Die erfassten Straßenzüge können so dreidimensional dargestellt werden. Das ULD meint, dass für diese personenbeziehbaren Messdaten ebenfalls die genannten Datenschutzanforderungen gelten. Widersprüche gegen die Veröffentlichung der Bilddaten schließen die im Laserscanverfahren erhobenen Daten mit ein.



Laserscan

Bei einem Laserscan werden Oberflächen zeilen- oder rasterartig durch einen Laserstrahl abgetastet. Das Verfahren wird eingesetzt, um Oberflächen oder Körper zu vermessen. Mit den erhobenen Daten können die vermessenen Objekte u. a. virtuell als Bild oder 3-D-Grafik dargestellt werden.

So ganz nebenbei teilte Google mit, anlässlich der Erfassung der Straßenzüge auch die **Daten privater WLAN-Funknetze** erhoben und gespeichert zu haben. Soweit uns bekannt ist, wurden georeferenzierte Angaben zu den MAC-Adressen der Access Points bzw. Router (BSSID), die Namen der Funknetze (SSID), der Verschlüsselungsstatus, die MAC-Adressen der in dem Funknetz angemeldeten Clients und sogenannte „Payload“-Daten erfasst. Zu letzteren gehören sämtliche Daten, die zum Zeitpunkt der Erfassung des Funknetzes in diesem technisch übermittelt wurden. Ein Großteil der gespeicherten Daten war verschlüsselt. Deren Inhalt kann daher durch Google nicht ausgewertet werden. Doch wurden auch unverschlüsselte Informationen auf den Festplatten des Unternehmens gefunden. Die vom Hamburgischen Beauftragten für den Datenschutz und Informationsfreiheit begonnene Untersuchung dauert an.

7.3 Stalking im Internet

Verfolgung und Belästigung betreffen auch die digitale Gesellschaft. Das ULD wird verstärkt um Beratung in Fällen gebeten, in denen Personen über das Internet belästigt und verleumdet wurden.

In diesen Fällen hatten die Angreifer detaillierte Kenntnisse über die verfolgten Personen. Die Angreifer nutzten die bei vielen Anbietern von Internetdiensten eher schwachen **Mechanismen zur Identitätsprüfung**. Häufiges Ziel sind die Profile der Betroffenen in sozialen Netzwerken. In mehreren Fällen veränderten die Angreifer bestehende Profile oder erstellten einfach konkurrierende oder neue Profile in Facebook, studiVZ oder meinVZ. Diese Profile wurden durch das Hintergrundwissen der Angreifer so gut mit Informationen gefüllt, dass Besuchern dieser Profile die Fälschung nicht auffiel.

Die Angreifer nutzten diese gefälschten Profile, um Bekannte, Freunde und Arbeitskollegen der Betroffenen zu kontaktieren und so das soziale Netzwerk der Person zu übernehmen. Daraufhin wurden im Profil z. B. **diffamierende Äußerungen** über die angebliche sexuelle Freizügigkeit der Betroffenen, finanzielle Probleme, laufende Strafverfahren oder Ähnliches verbreitet. Für die Betroffenen haben diese Angriffe weitreichende Konsequenzen; sie stellen oft eine unerträgliche Belastung der familiären und beruflichen Beziehungen dar.

Zunächst raten wir allen Betroffenen, bei der zuständigen Polizeidienststelle Anzeige zu erstatten. Die Anbieter von sozialen Netzwerken reagieren häufig nach Kenntnisnahme solcher Angriffe mit dem **simplen Löschen** der kompromittierenden Inhalte. Dies hilft oft aber nur kurzfristig, weil die Angreifer schnell ein neues Profil unter gleichem Namen erstellen oder eine andere Plattform nutzen.

Gerade wegen des hohen Schadens, den eine Profilfälschung in sozialen Netzwerken anrichten kann, fordert das ULD von den Betreibern eine deutlich **bessere Authentifizierung** der Nutzerinnen und Nutzer. Zumindest sollten von solchen Angriffen betroffene Personen technische und organisatorische Hilfen zum Selbstschutz erhalten. Schnelle Abhilfe brächten Prüflisten bei den Anbietern, die beim Anlegen eines neuen Profils unter demselben Namen eine manuelle Prüfung durch den Anbieter erfordern.

Das ULD unterstützt in den vorliegenden Fällen die zuständigen **Strafverfolgungsbehörden** und arbeitet auf einen regelmäßigen Erfahrungsaustausch hin. Wir werden die Anbieter von Diensten mit erhöhtem Gefahrenpotenzial des digitalen Stalkings mit den Vorfällen konfrontieren und zur Umsetzung besserer Sicherheitsmaßnahmen auffordern.

Was ist zu tun?
Anbieter von sozialen Netzwerken müssen ihre Nutzer vor Profildiebstahl und Profilfälschung besser als bisher schützen. Ein einfaches Löschen reicht nicht. Das ULD unterstützt die Strafverfolgungsbehörden durch Beratung und wird versuchen, zusammen mit den Anbietern bessere Schutzmaßnahmen für die Nutzer zu finden.

8 Modellprojekte und Studien

Neben seiner Prüf- und Beratungstätigkeit beteiligt sich das ULD an **drittmittelfinanzierten Projekten und Studien** mit besonderem Datenschutzbezug. Ziel ist es, über das gesetzlich notwendige Mindestmaß an Datenschutz hinauszugehen und besonders „datenschutzfördernde Technik“ zu entwickeln, die den Bürgerinnen und Bürgern in Schleswig-Holstein zugutekommt. Auch im vergangenen Jahr ist das ULD an einer Reihe von Projekten und Studien beteiligt gewesen, die durch Drittmittel finanziert wurden (Tz. 8.1 bis Tz. 8.7).



Koordiniert werden solche Projekte innerhalb unseres **Innovationszentrums Datenschutz & Datensicherheit (ULD-i)**, das interessierten schleswig-holsteinischen Unternehmen und Hochschulen für die Implementierung von Datenschutz und Datensicherheit in ihre Projekte und Produkte zur Verfügung steht.

 http://www.uld-i.de/

Im Dezember 2010 wurde das **Virtuelle Datenschutzbüro** als gemeinsames Internetportal der Datenschutzaufsichtsbehörden zehn Jahre alt. Die Geschäftsleitung wird auch weiterhin beim ULD liegen. Als Projekt gestartet, ist es heute mit etwa 3.000 Beiträgen und Artikeln eine der wichtigsten Informationsquellen zum Datenschutz im deutschsprachigen Raum. Täglich besuchen das Portal inzwischen mehr als 3.400 Nutzerinnen und Nutzer.

 https://www.datenschutz.de/

8.1 PrimeLife – Identitätsmanagement im Fokus

Das von der EU geförderte Projekt PrimeLife verfolgt das Ziel, Menschen in ihrer informationellen Selbstbestimmung durch nutzergesteuertes Identitätsmanagement zu unterstützen. Wie dies geht, zeigen erste Prototypen.

> **?** ***Identitätsmanagement***
>
> *Identitätsmanagement ist ein von den Menschen seit Jahrhunderten eingeübtes Handeln: Man verhält sich je nach Situation oder Rolle verschieden und gibt unterschiedliche Informationen von sich preis.Im Internet ist ein solches instinktives Management seiner verschiedenen Teilidentitäten schwierig. Hierbei können Identitätsmanagementsysteme unterstützen, die z. B. pseudonyme Kennungen für verschiedene Anbieter vorsehen. Wichtig ist, dass die Nutzer die Kontrolle über ihre Daten und deren Verwendung ausüben können.*

Während 2004 bis 2008 mit ULD-Beteiligung im durchgeführten Vorgängerprojekt „PRIME – Privacy and Identity Management for Europe“ an einem umfassenden Prototyp mit möglichst viel Funktionalität gearbeitet

wurde, konzentriert sich das PrimeLife-Projekt auf einzelne Module und Tools, die in Kombination mit existierenden Systemen und Anwendungen zum Einsatz kommen können. Unsere Rolle besteht in der **datenschutzrechtlichen Analyse und Konzeption** von rechtskonformen und gleichzeitig praktikablen sowie bedienfreundlichen Lösungen (32. TB, Tz. 8.2).



Ein Schwerpunkt von PrimeLife liegt im Bereich der **sozialen Netzwerke**. Mit dem Prototyp „Clique" wurde ein eigenes soziales Netzwerk mit besonderer Datenschutzfunktionalität entwickelt. Insbesondere ermöglicht es den Nutzern, unter ihren Profilen mehrere Teilidentitäten anzulegen und jeweils zu bestimmen, wer auf die Daten Zugriff hat, seien es Freunde, Familie, Arbeitskollegen oder Geschäftskontakte. Da allerdings auch bei diesem System der Betreiber des sozialen Netzwerks in seiner zentralen Sicht den „sozialen Graphen", d. h. wer mit wem in welcher Beziehung steht, ermitteln kann, wird zusätzlich an dezentralen Lösungen gearbeitet.

Bereits jetzt einsetzbar ist die Browsererweiterung „Scramble!", mit der sich Inhalte in sozialen Netzwerken **ver- und entschlüsseln** lassen. Nur wer im Besitz des passenden Schlüssels ist, sieht dann Klartext in den Profilfeldern einer Person. Ebenso können Nachrichten verschlüsselt und digital signiert werden.

Nützlich für jedes Surfen im Internet ist das ebenfalls als Browsererweiterung realisierte „Privacy Dashboard" von PrimeLife. Damit können Nutzer nachvollziehen, welche ihrer Nutzungsdaten vom Webseitenanbieter oder Dritten gesammelt werden (z. B. über verschiedene Arten von Cookies), und den Umgang mit Cookies oder das Ausführen von Scripts auf einfache Weise konfigurieren. Auf diese Weise kann der Nutzer ungewollter **Profilbildung oder Aufzeichnung** des Nutzungsverhaltens entgegenwirken und zugleich die Möglichkeiten der Verkettbarkeit verringern. Diese und weitere PrimeLife-Tools stehen als **Open-Source-Software** zum Download auf der Webseite des Projekts zur Verfügung.



http://www.primelife.eu/results/opensource/

Was ist zu tun?
PrimeLife stellt mit seinen Prototypen unter Beweis, dass in heutigen Anwendungen mehr Datenschutzfunktionalität machbar ist. Anbieter von Internetdiensten sollten prüfen, inwieweit sie mit PrimeLife-Tools oder eigenen Entwicklungen mehr Datenschutz in ihren Anwendungen realisieren können.

8.2 ABC4Trust – Pilot für eine vertrauenswürdige digitale Identifikation

Seit November 2010 läuft das von der Europäischen Union für vier Jahre geförderte Projekt „ABC4Trust – Attribute-Based Credentials for Trust“. Ziel ist die praktische Erprobung von datensparsamen Berechtigungsnachweisen in der digitalen Welt.

Das gesetzlich festgeschriebene **Gebot zur Datensparsamkeit** ist in der Praxis manchmal schwer umzusetzen, wenn zugleich ein Mindestmaß an Sicherheit erforderlich ist. Beispielsweise enthalten die zur Legitimation eines Kunden verwendeten Dokumente zumeist mehr Daten, als für den konkreten Zweck preisgegeben werden müssten. So erfährt ein Händler bei Vorlage einer Studienbescheinigung neben der Eigenschaft „Person ist Student“ oft auch Name, Adresse, Geburtsdatum und Studienfach als quasi aufgedrängte Informationen. Besteht bei einem Ausweis in Papierform noch die Möglichkeit, einzelne Felder beim Kopieren zu schwärzen oder beim Vorzeigen abzudecken, ist dies online mit vom Aussteller digital signierten Nachweisen, also von Zertifikaten, bisher nicht möglich: Bei einmal vom Aussteller erteilten Zertifikaten kann der Inhalt nicht variiert werden, denn herkömmliche digitale Signaturen verlieren ihre Gültigkeit, sobald auch nur ein Teil der signierten Informationen entfernt oder geändert wird.

Anders ist dies bei **attributbasierten Nachweisen**, den „Attribute-Based Credentials“, die es ermöglichen, einzelne Attribute zu bescheinigen, z. B. Name, Studenteneigenschaft oder Geburtsdatum. Nutzer können dann die erforderlichen Angaben selbst in einem neuen Zertifikat zusammenstellen und dieses übermitteln. Die Signatur und damit die Bescheinigung des Ausstellers, dass die Angaben korrekt sind, bleibt erhalten, sogar für durch Berechnungen abgeleitete Eigenschaften wie das aus dem aktuellen Datum und dem Geburtstag zu errechnende Alter einer Person. Attribute-Based Credentials erlauben es so, datensparsam bestimmte Eigenschaften gegenüber Dritten nachzuweisen, ohne die eigene Identität zu offenbaren.

Das Projekt ABC4Trust wird die beiden bereits bestehenden Software-Implementierungen von Attribute-Based Credentials, namentlich IBM Identity Mixer (Idemix) und Microsoft U-Prove, **im Rahmen zweier Piloten erproben**. In einem Piloten werden Schüler, Eltern und Kollegium einer weiterführenden Schule in Schweden die Technologie verwenden, um sich gegenseitig auf der schulinternen Kommunikationsplattform zu authentifizieren. Im zweiten Piloten nutzen Studenten der griechischen Universität Patras die Technologie zur Bewertung der Lehre. Als Teilnehmer von Veranstaltungen erhalten sie Credentials, um später nur die Vorlesungen bewerten zu können, an denen sie teilgenommen haben.

Da die bestehenden Credential-Systeme Idemix und U-Prove auf unterschiedlichen kryptografischen Algorithmen beruhen, kann man sie nicht einfach zusammenschalten. Ziel des ABC4Trust-Projekts ist die Entwicklung einer Architektur, die es ermöglicht, **Credentials interoperabel** einzusetzen. Wir legen dabei den Fokus auf die datenschutzrechtlichen Aspekte. Das Projektkonsortium besteht neben dem ULD aus Partnern aus Industrie – IBM, Microsoft, Nokia Siemens

Networks −, Wissenschaft und Pilotanwendern. ABC4Trust wird vom Lehrstuhl für Mobile Business & Multilateral Security an der Universität Frankfurt geleitet.



http://www.abc4trust.eu/

Was ist zu tun?
Innovative datenschutzfördernde Technologien schützen die Privatsphäre von Nutzern und Geschäftspartnern, wenn sie bestimmte Berechtigungen nachweisen müssen. Bei der Planung und Inbetriebnahme neuer Verfahren sollten diese Techniken berücksichtigt werden.

8.3 TClouds – auf dem Weg zum vertrauenswürdigen Cloud Computing

„TClouds – Trustworthy Clouds“ heißt ein Projekt, in dem unter Beteiligung des ULD eine sichere und datenschutzgerechte Cloud-Computing-Infrastruktur entwickelt werden soll. Das Projekt startete im Oktober 2010 und wird für die Dauer von drei Jahren von der Europäischen Union gefördert.

„Cloud Computing lässt sich übersetzen mit „Datenverarbeitung in der Wolke“. Diese „Wolke“ beschreibt eine für die Anwender **fremde, zumeist uneinsehbare informationstechnische Infrastruktur**, in die sie eigene Datenverarbeitungsprozesse über das Internet auslagern können. Die Nutzung dieser fremden Ressourcen erlaubt es, nach der tatsächlichen Nutzung von Rechenleistung und -zeit abzurechnen und somit Kosten für das Bereithalten und die Pflege einer eigenen technischen Infrastruktur einzusparen.

? *Cloud Computing*

Cloud-Computing-Infrastrukturen sind ein Angebot von bedarfsgerechten informationstechnischen Dienstleistungen, die über das Internet in Form von Speicher- oder Rechenleistung, Entwicklungsumgebungen, Anwendungssoftware oder sogar vollständigen Arbeitsumgebungen bereitgestellt werden. Die Daten der Anwender werden hierbei nicht lokal im eigenen Verfügungsbereich gespeichert und verarbeitet, sondern in einer sogenannten „Datenwolke“, auf die die Anwender über das Internet zugreifen. Für die Anwender bleibt dabei unklar, was genau mit ihren Daten geschieht.

Cloud Computing wird bereits von zahlreichen Firmen genutzt, um ganze Arbeitsprozesse in die Cloud auszulagern oder um Bedarfsspitzen abzudecken, mit denen die eigene technische Infrastruktur überfordert wäre. Auch Privatleute haben die Möglichkeit, Angebote aus der Cloud zu nutzen.

Aus Sicht der Anwender findet die eigentliche Datenverarbeitung in der Cloud **intransparent** statt: Sie haben in der Regel keine Kenntnis davon, wo genau sich ihre Daten in der „Wolke“ befinden, wer Zugriff auf diese hat, wo sie physisch gespeichert werden und ob die Datenschutz- und Datensicherheitsmaßnahmen des Cloud-Anbieters den gesetzlichen und ihren eigenen organisationsinternen Anforderungen entsprechen. Da viele Anbieter von Cloud Computing international agierende Unternehmen mit Servern außerhalb Europas sind, stellt dies insbeson-

dere für europäische Anwender ein Hindernis dar, die ihrer Verantwortung für die Datenverarbeitung gemäß dem EU-Rechtsrahmen nachkommen müssen.

TClouds will diese Probleme mithilfe einer **transparenten und vertrauenswürdigen Infrastruktur** für solche Angebote lösen. Diese soll Anwendern eine grenzüberschreitende und dennoch datenschutzgerechte und sichere Datenspeicherung und -verarbeitung ermöglichen und zugleich die wirtschaftlichen Vorteile der bisherigen Cloud-Computing-Lösungen beibehalten.

Die TClouds-Konzepte werden im Laufe des Projekts anhand **von Szenarien im Gesundheitsbereich sowie im Energiesektor** erprobt. Beide Einsatzbereiche sind beispielhaft hinsichtlich der unterschiedlichen Sensibilität der zu verarbeitenden Daten und der Anforderungen an das Sicherheitsniveau der Cloud.


http://www.tclouds-project.eu/

Was ist zu tun?
Jeder, der personenbezogene Daten in einer Cloud verarbeiten möchte oder eine Cloud-Computing-Infrastruktur aufbaut, muss dabei die datenschutzrechtlichen Anforderungen einhalten. Dies gilt insbesondere für grenzüberschreitende Datenflüsse sowohl innerhalb als auch außerhalb der Europäischen Union.

8.4 AN.ON – Anonymität.Online

Das ULD bietet weiterhin einen kostenlosen Anonymisierungsserver an, der zusammen mit anderen Anbietern eine Grundversorgung an Anonymität im Internet gewährleistet.

Infolge des Urteils des Bundesverfassungsgerichts vom März 2010 zur Unzulässigkeit der Regelungen zur **Vorratsdatenspeicherung** haben wir umgehend die Aufzeichnung von Verbindungsdaten auf unserem Anonymisierungsserver abgeschaltet und die entsprechenden Protokolle gelöscht. Auch die übrigen Betreiber sind nach unserem Wissen entsprechend verfahren.

Unser Server wird weiterhin gleichzeitig von **ca. 1.200 Nutzern** im Rahmen von „AN.ON – Anonymität.Online" für den anonymen Zugriff von Webseiten eingesetzt (32. TB, Tz. 8.6). Die Anfragen von Strafverfolgungsbehörden wegen Missbrauchs sind gegenüber den letzten Jahren deutlich zurückgegangen.


http://www.anon-online.de/

Was ist zu tun?
Das ULD wird die Gesetzgebung zur Vorratsdatenspeicherung beobachten und bei Bedarf den Anonymisierungsdienst an neue Regelungen anpassen. Den Bürgern ist auch künftig im Rahmen der rechtlichen Vorgaben eine kostenlose Möglichkeit zur anonymen Nutzung des Internets zur Verfügung zu stellen.

8.5 Studie zu Datenschutz in Online-Spielen veröffentlicht

Das Projekt „DOS – Datenschutz in Online-Spielen wurde Ende 2009 abgeschlossen. Das ULD hat nun die Studie und einen Leitfaden zur datenschutzgerechten Entwicklung von Online-Spielen aktualisiert und veröffentlicht.

Das DOS-Projekt wurde von 2007 bis 2009 vom Bundesministerium für Bildung und Forschung gefördert (32. TB, Tz. 8.5). Hierbei haben wir Online-Spiele für PCs, Konsolen, Handhelds, Handys, Browser und soziale Netzwerke untersucht und die wichtigsten Datenschutzprobleme identifiziert. Auf der Basis unserer Analyse haben wir einen Leitfaden für Entwickler und Betreiber von Online-Spielen zusammengestellt, der Rechtsgrundlagen, Problembereiche und **praktische Tipps** zur Umsetzung des Datenschutzes in solchen Spielen aufzeigt. Die umfangreiche Studie und der Leitfaden können kostenlos von unserer Webseite heruntergeladen werden.



https://www.datenschutzzentrum.de/dos/

Zahlreiche Anfragen von Spielern, Jugendorganisationen, Herstellern und Betreibern von Online-Spielen infolge der Veröffentlichung zeigen das große Interesse an diesem aktuellen Thema. Bei vielen ist die **Unsicherheit** groß, wie Datenschutz in Online-Spielen umzusetzen ist. Hier können die Studie und der Leitfaden eine Orientierung geben.

Was ist zu tun?
Das ULD wird die weiteren Entwicklungen im Bereich der Online-Spiele beobachten. Dies gilt insbesondere für neue Techniken, z. B. die Einbindung von Videobildern und das Zusammenspiel mit sozialen Netzwerken. Für ein Fortschreiben des Leitfadens suchen wir Kooperationspartner.

8.6 RISERid – Registry Information Service on European Residents Initial Deployment

Das Projekt zur europäischen Melderegisterauskunft RISER macht im sechsten und letzten Projektjahr vor, wie Datenschutz in einem E-Government-Verfahren erfolgreich umgesetzt werden kann.



Das seit März 2004 entwickelte und von der Europäischen Kommission im Rahmen des eTEN-Programms geförderte Verfahren zur **elektronischen Melderegisterauskunft** hat sich als Innovationsmotor im Bereich der Vermittlung datenschutzgerechter Melderegisterauskünfte auf europäischer Ebene etabliert. Die EU-Förderung läuft Anfang 2011 aus; das Projekt ist aber längst wirtschaftlich etabliert und erfolgreich und zeigt, dass datenschutzfreundliche Lösungen im Wettbewerb Bestand haben können.

Die datenschutzgerechte Ausgestaltung des seit 2007 von der RISERid Services GmbH betriebenen Dienstes stand immer mit im Fokus. RISER leitet elektroni-

sche Anfragen an Einwohnermeldebehörden **in zehn europäische Länder** weiter. Bis zu 200.000 Anfragen an Meldebehörden werden bei RISER monatlich zentral angefragt und abgeholt. Slowenien und Finnland werden in Kürze hinzukommen. Die Reichweite für elektronische Anfragen in Deutschland erreichte 80 % im Jahr 2010. In Europa werden 246 Millionen Einwohner erreicht, das sind 52 % der Einwohner. Der Dienst bietet seinen Kunden einen einheitlichen Zugang zu einer sehr heterogenen und unübersichtlichen Melderegisterlandschaft in Europa. Über das Serviceportal werden Meldeanfragen als Datei- oder Einzelanfrage über das Internet an die zuständige Meldebehörde weitergeleitet. RISER übernimmt die Funktion eines Zustellers. Als **Auftragsdatenverarbeiter** verwendet der Dienst die personenbezogenen Daten ausnahmslos zu den vertraglich festgelegten Zwecken und verarbeitet sie nach den vertraglich festgelegten datenschutzkonformen Verfahren. Auskünfte werden ausschließlich fallbezogen für den jeweiligen Kunden verarbeitet und die Ergebnisse ausschließlich für diesen bereitgehalten. RISER speichert keine Ergebnisse aus Melderegisterauskünften für eigene Zwecke und macht sie weder Dritten zugänglich noch überführt Adressen in einen sogenannten Treuhandpool. Damit schützt RISER Einwohnermeldedaten strenger, als dies in einigen anderen Bundesländern der Fall ist. Diese Länder erlauben die Weiterverwendung von Einwohnermeldeauskünften, die durch Anfragen für Auftraggeber im Rahmen der Auftragsdatenverarbeitung erlangt wurden. Dies ist aus Datenschutzsicht heikel, insbesondere wenn der Auftraggeber z. B. eine Bundesanstalt ist. Allein über die Tatsache der Anfrage durch diesen Auftraggeber besteht eine Zusatzinformation, die, wird sie dem Meldedatensatz angefügt, zu negativen Auswirkungen für den betroffenen Bürger führen kann.

Das Angebot von RISER unterscheidet sich positiv durch die strikte Zweckbindung im Rahmen der Auftragsdatenverarbeitung von dem Angebot vieler Adresshändler und Auskunfteien. Insbesondere das Sammeln von Adressen in sogenannten **Adressen- oder Treuhandpools** (32. TB, Tz. 8.7) zur Weiterverwendung ist datenschutzrechtlich problematisch und allenfalls zulässig, wenn der Addresssammler oder Treuhandpool sich seinerseits auf eine eigene Rechtsgrundlage für die Datenverarbeitung berufen kann. Eine Datenverarbeitung im Auftrag liegt in diesen Fällen in der Regel nicht vor, denn der „Treuhänder" speichert die Daten für eigene Zwecke. Die Einstellung der im Rahmen einer einfachen Melderegisterauskunft erlangten Adressdaten in den Pool erfüllt nicht mehr den vom Auftraggeber verfolgten Geschäftszweck. Der Auftraggeber hat die gewünschte Auskunft erhalten, und der Vorgang ist abgeschlossen. Die weitere Vorhaltung der Daten ist für diesen Auftrag nicht mehr erforderlich und dient ausschließlich dem Dienstleister, der aus dem Pool der gespeicherten Adressen andere anfragende Stellen beauskunftet. Die Geschäftszwecke des Auftraggebers können nicht als Rechtsgrundlage für eine Auftragsdatenverarbeitung und den Aufbau eines treuhänderisch verwalteten Datenpools herangezogen werden.

Auch das über RISER bei einer Meldebehörde anfragende Unternehmen darf die durch die Meldeauskunft aktualisierte Adresse nur dann für Zwecke der **Werbung, Markt- oder Meinungsforschung** nutzen, wenn diese Nutzung ebenfalls durch eine Rechtsgrundlage abgedeckt und insoweit nach dem Bundesdatenschutzgesetz zulässig ist.

Bei der einfachen Melderegisterauskunft, die durch die deutschen Meldebehörden an Anfragende nur bei Nennung von Namen und Adresse oder Geburtsdatum über eine dadurch eindeutig zu identifizierende Person erteilt wird, handelt es sich um eine **nicht allgemein zugängliche Quelle**. Die einfache Meldeauskunft wird nicht voraussetzungslos erteilt: Der Anfragende muss im berechtigten Besitz eines Datensatzes sein, mit dem die gesuchte Person eindeutig identifizierbar ist; schutzwürdige Interessen der betroffenen Person dürfen der Auskunft nicht entgegenstehen.

Im Mai 2010 fand die **5. Konferenz für E-Services im Meldewesen in Europa** im Rathaus Schöneberg in Berlin statt. 120 internationale Teilnehmer aus 21 Ländern diskutierten über Melderecht und Datenschutz bei nationalen Melderegistern. Auf der Konferenz stellte die Organization for Security and Cooperation in Europe (OSCE) ihren Leitfaden zum Melderecht vor. Die Konferenz wird sich weiterhin als Forum für Interessenvertreter aus dem Bereich Meldewesen mit lokalen, nationalen, europäischen und insbesondere mit datenschutzrechtlichen Fragen befassen. Mit einer Veranstaltung im Februar 2011 zum Thema „Vorteil Datenschutz – Wie Unternehmen und Behörden Datenschutz zu ihrem Vorteil nutzen können“ wurde das RISER-Projekt abgeschlossen.



http://www.riserid.eu/

8.7 Datenschutzdiskurse im „Privacy Open Space“

Das Projekt „Privacy Open Space“ – kurz „PrivacyOS“ – wurde vom ULD initiiert, um unterschiedliche Akteure aus den Bereichen IT-Entwicklung und Datenschutz zusammenzubringen und Lösungsvorschläge für drängende Probleme vorzustellen und zu diskutieren.



Die Erfahrungen von Entwicklern, Nutzern und Datenschutzbehörden zeigen, dass die Anforderungen des Datenschutzes bei E-Services bereits in einem frühen Stadium berücksichtigt, umgesetzt und in Prozesse integriert werden müssen. Es fehlten Foren für die Beteiligten zur Diskussion aktueller und richtungsweisender Entwicklungen. Diese Lücke wurde von PrivacyOS geschlossen. Das ULD erhielt 2008 hierfür den Zuschlag im Rahmen des „ICT Policy Support Programme“ der Europäischen Kommission. Das Projekt führte Vertreter aus den Bereichen **Wirtschaft, Wissenschaft, Regierung und Gesellschaft** zusammen, um die Entwicklung und die Anwendung von Datenschutzinfrastrukturen in Europa zu fördern und zu unterstützen. Alle 15 Projektpartner aus 12 europäischen Ländern und das ULD als Koordinator können langjährige Erfahrungen auf dem Gebiet des Datenschutzes aufweisen.

Der Datenschutzdiskurs auf den Konferenzen von PrivacyOS erfolgt nach der sogenannten **Open-Space-Methode**: Die Teilnehmerinnen und Teilnehmer bringen eigene Themen ein und gestalten dazu Vorträge und Diskussionen. Die

Agenda eines Open Space, also eines offenen Raums, wird erst zu Beginn einer Konferenz erstellt. Jeder kann ein Datenschutzthema einbringen und bekommt in Abhängigkeit des Interesses der anderen Teilnehmer einen Zeitblock und einen Raum zugeordnet. Diese Dynamik erleichtert es, neue und aktuelle Themen zu behandeln. Ziel ist die Etablierung einer dauerhaften Zusammenarbeit und des Austausches innerhalb der Mitgliedstaaten und verschiedener EU-Projekte zum Thema Datenschutz.

PrivacyOS ist ein **Diskussionsforum für Best Practices** zu Themen wie Electronic ID-Cards, eParticipation, Datenschutz-Gütesiegel oder Kryptomechanismen. Über einen Zeitraum von zwei Jahren wurden vier Open-Space-Konferenzen parallel zu Veranstaltungen mit datenschutzrechtlicher Relevanz für Vertreter aus den Bereichen Wirtschaft, Wissenschaft, Regierung und Gesellschaft angeboten.

Nach den ersten drei PrivacyOS-Konferenzen in Straßburg (2008), Berlin und Wien (beide 2009) mit regem internationalem Zuspruch (32. TB, Tz. 8.8) fand die letzte im Rahmen des geförderten Projektes abgehaltene **Veranstaltung in Oxford** mit 61 Teilnehmern aus 15 Ländern statt. Vertreten waren die Organisationen W3C, der Europäische Verbraucherverband (beuc), die Universitäten Frankfurt und Leipzig, Nokia Siemens, HP, die Datenschutzbehörde aus Litauen sowie Teilnehmer aus den Vereinigten Staaten und Japan. Schwerpunkte bei den 30 Vorträgen in Oxford waren die Erhöhung des Datenschutzbewusstseins und Möglichkeiten der besseren Sichtbarmachung von datenschutzrelevanten Aspekten bei der Online-Nutzung über Datenschutzsymbole, sogenannte Privicons, die Überwachung und Verfolgung, also das Tracking von Online-Aktivitäten durch den Staat oder private Unternehmen – z. B. beim digitalen Fernsehen, durch Google Street View, in sozialen Netzwerken – und die Steuerung im häuslichen Bereich, z. B. durch RFID.

Als Resultat der Konferenzreihe wurde ein **Open-Space-Leitfaden** erstellt, der die in dem Projekt gesammelten Erfahrungen für die Organisation zukünftiger Konferenzen zur Verfügung stellen soll. Die Konferenzen erwiesen sich als Motor für die Zusammenarbeit der Akteure bei der Weiterentwicklung des technischen und rechtlichen Datenschutzes. Es wird angestrebt, die aufgebauten Kontakte über eine projektbezogene Zusammenarbeit fortzuführen und den Open-Space-Ansatz bei zukünftigen Veranstaltungen als Angebot aufzunehmen.


https://www.privacyos.eu/

Was ist zu tun?
Die Vernetzung und Kommunikation unter den Akteuren ist weiter zu verbessern, um einen proaktiven Datenschutz in privaten und öffentlichen Organisationen zu unterstützen und umzusetzen.

9 Audit und Gütesiegel

9.1 Datenschutz-Audits

9.1.1 BSI-Zertifizierung für die Kreisverwaltung Plön

Der Kreis Plön ist der erste Landkreis in Schleswig-Holstein, dessen IT-Sicherheitsmanagement vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert wurde.

> ***? ISO 27001***
>
> *Internationale Norm für das Management von IT-Sicherheit.*
>
> ***? ISO 27001 auf der Basis von IT-Grundschutz***
>
> *Kombination der Vorgaben der Norm ISO 27001 für das Sicherheitsmanagement mit detaillierten materiellen Sicherheitsmaßnahmen der IT-Grundschutzkataloge.*

Die Kreisverwaltung Plön ist unter den Kommunen des Landes schon lange ein Vorreiter im Bereich Datenschutz und IT-Sicherheit. Die **Basisinfrastruktur** der Kreisverwaltung, über die zentralisiert alle Fachverfahren und die Kommunikation mit anderen Netzen, z. B. dem Internet und dem Kreisnetz, abgewickelt werden, wurde nach den IT-Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgerichtet. Sie umfasst den zentralen Betrieb aller Anwendungsprogramme auf Terminalservern und die Datenspeicherung in zwei redundanten Serverräumen. Im Oktober 2010 bescheinigte das BSI dem Kreis Plön, dass das IT-Sicherheitsmanagement der Basisinfrastruktur den Vorgaben der ISO-Norm 27001 auf der Basis von IT-Grundschutz (32. TB, Tz. 9.2.1) entspricht. Die Basis dieser Zertifizierung bildete eine Prüfung durch Auditoren des ULD, die sich von der Funktionsfähigkeit des IT-Sicherheitsmanagements und der Sicherheitsmaßnahmen überzeugt haben. Dazu wurde die Dokumentation des IT-Sicherheitsmanagements analysiert und die im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen auf Plausibilität geprüft. Im nächsten Schritt wurde vor Ort stichprobenartig kontrolliert, ob die Sicherheitsmaßnahmen wie vorgesehen implementiert und wirksam waren. Schließlich überprüfte das BSI als Zertifizierungsstelle den von den Auditoren erstellten Prüfbericht auf Plausibilität und Vollständigkeit.

Das Zertifizierungsverfahren hat ein **dauerhaft hohes Sicherheitsniveau** zum Ziel. Während der dreijährigen Laufzeit der Zertifizierung erfolgen im Jahresrhythmus zwei Überwachungsaudits, bei denen das IT-Sicherheitsmanagement sowie die sichere Einbindung von neuen und geänderten IT-Systemen überprüft wird.

> **Was ist zu tun?**
> Die IT-Abteilung des Kreises Plön sollte für andere Kommunalverwaltungen Leitbild bei der Umsetzung von IT-Sicherheit und Datenschutz werden. Durch die Zertifizierung wurde ein hohes IT-Sicherheitsniveau erreicht, das auch zukünftig zu halten ist.

9.1.2 Stadt Bad Schwartau

Bad Schwartau ist die erste Kommune, die sich einer fortlaufenden regelmäßigen Datenschutzüberprüfung durch das ULD unterzieht. Damit setzen die Verantwortlichen Maßstäbe und gewährleisten Datenschutz und Datensicherheit auf hohem Niveau.



Bereits **zum dritten Mal** hat das ULD der Stadtverwaltung Bad Schwartau das Datenschutzauditzeichen für eine vorbildliche und ordnungsgemäße Datenverarbeitung verliehen. Schon 2004 hatte sie ihr hohes Niveau an Datensicherheit bei der Verarbeitung ihrer Bürgerdaten auf EDV-Systemen von uns auditieren lassen. Im Jahr 2007 wurde die Aufrechterhaltung des Sicherheitsniveaus erfolgreich reauditiert. Auf der Basis eines entsprechenden Auftrags kontrollierte das ULD die Datensicherheit in Bezug auf Wirkungsweise und Beständigkeit erneut umfassend und bescheinigte der Stadtverwaltung, dass sie das Datenschutzauditzeichen für weitere drei Jahre führen darf.

In einem Datenschutzkonzept sind für die automatisierte Datenverarbeitung und den Anschluss des Verwaltungsnetzes an das Internet Sicherheitsmaßnahmen festgelegt, die auf ihre **Umsetzung und Wirkungsweise** überprüft wurden. Die IT-Koordinatoren haben auf der Basis von Windows-Terminalservern eine zentrale Verwaltung der Fachanwendungen und der Daten realisiert. Die Sicherheit an den Arbeitsplatzrechnern wird so deutlich erhöht, weil die Datenverarbeitung nur noch auf den zentralen Rechnern erfolgt. Außerdem werden die E-Mail-Kommunikation und die Nutzung des WWW vor unerwünschten Ereignissen durch den Einsatz mehrerer aufeinander aufbauender Sicherheitsmechanismen geschützt.

Was ist zu tun?
Bad Schwartau sollte seine Vorbildfunktion für andere kommunale Verwaltungen erhalten und deutlich machen, welche Vorteile sich durch geregelte Datenschutz- und IT-Sicherheitsprozesse ergeben.

9.1.3 ZIAF-Audit

Das Ministerium für Landwirtschaft, Umwelt und ländliche Räume erhielt für die sichere Konzeption und den sicheren Betrieb seiner Agrarförderungszahlstelle ein IT-Sicherheitszertifikat. Im April 2010 wurde das erste turnusmäßige Überwachungsaudit ohne Beanstandungen abgeschlossen.

Zur Erinnerung: Die Europäische Union (EU) hat für Zahlstellen, die EU-Fördermittel für die Agrarförderung auszahlen, sicherheitstechnische Vorgaben gemacht, um Ausfällen der Informationstechnik und Manipulationen vorzubeugen. Im Jahr 2007 wurde die **Konzeption** des IT-Sicherheitsmanagements beim Ministerium für Landwirtschaft, Umwelt und ländliche Räume (MLUR) und dem beteiligten Dienstleister Dataport in zwei Datenschutz-Audits überprüft (30. TB, Tz. 9.1.1). Grundlage war dabei die IT-Sicherheitsnorm ISO 27001 auf der Basis von IT-Grundschutz (Tz. 9.1.1).

Nun hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die **Umsetzung** dieser Konzeption zertifiziert (32. TB, Tz. 9.2.4). Damit ist das MLUR zu jährlichen Überprüfungen durch einen anerkannten BSI-Auditor im Rahmen von sogenannten Überwachungsaudits verpflichtet, um einen hohen IT-Sicherheitsstandard innerhalb der dreijährigen Gültigkeitsdauer des Zertifikats nachzuweisen. Dabei wird überprüft, ob das IT-Sicherheitsmanagement weiterhin wirksam ist und ob Änderungen an den IT-Systemen oder der Organisation so erfolgen, dass die IT-Sicherheit weiterhin gewährleistet ist. Das erste Überwachungsaudit wurde erfolgreich abgeschlossen.

Was ist zu tun?
Das MLUR plant, das IT-Sicherheitsmanagement auf weitere Bereiche auszudehnen. Die Weiterverwendung von Konzepten erlaubt das Heben des Sicherheitsniveaus auf rationelle Art. Ausreichende Ressourcen sind nötig, um den erreichten Sicherheitsstandard dauerhaft zu gewährleisten.

9.1.4 Zensus 2011

Das Statistikamt Nord beauftragte das ULD mit einer kritischen Analyse der IT-Sicherheit für die Datenverarbeitung des Zensus 2011 und mit der beratenden Unterstützung bei der Festlegung von organisatorischen und technischen Sicherheitsmaßnahmen.

Die Europäische Union (EU) hat für das Jahr 2011 eine gemeinschaftsweite Volks-, Gebäude- und Wohnungszählung – den Zensus 2011 – angeordnet. Dabei wird in Deutschland ein neues Verfahren eingeführt, das sich grundlegend von traditionellen Volkszählungen unterscheidet.

Beim **registergestützten Zensus** werden hauptsächlich vorhandene Verwaltungsregister wie z. B. das Melderegister genutzt. Nach dem Zensusstichtag, dem 9. Mai 2011, werden die Daten aus den verschiedenen Registern und den Befragun-

gen mit einem statistischen Verfahren – der sogenannten Haushaltsgenerierung – zusammengeführt. Am Ende der Erhebung und Aufbereitung liegen zuverlässige Zensusdaten zu Personen, Haushalten, Wohnungen und Gebäuden vor.

Das Statistikamt Nord wird von uns bei der Einrichtung der Datenverarbeitungsprozesse und der umzusetzenden organisatorischen und technischen Sicherheitsmaßnahmen unterstützt. Im Rahmen eines Audits wird die durchzuführende Verarbeitung dem Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in den Schritten der Grundschutzmethode unterzogen. Es wurden die für die Durchführung des Zensus erforderlichen infrastrukturellen und technischen Bereiche geordnet, der Schutzbedarf der Daten ermittelt, die Sicherheitsmaßnahmen festgelegt und überprüft sowie Restrisiken bewertet. Das Statistikamt ist auf einem guten Weg, alle erforderlichen **Sicherheitsanforderungen bis zum Stichtag** im Mai 2011 zu erfüllen.

Was ist zu tun?
Das Statistikamt Nord sollte seine strategische Ausrichtung, den Datenschutz und die IT-Sicherheit nach dem Grundschutzstandard für die Zensusdatenverarbeitung umzusetzen, konsequent fortentwickeln.

? *Zensus 2011*

Im Jahr 2011 findet in Deutschland nach über 20 Jahren eine Zählung der Bevölkerung und der Wohnungen statt. Die aktuellen Bevölkerungs- und Wohnungszahlen basierten auf Fortschreibungen der jeweils letzten Volkszählung, die in der Bundesrepublik Deutschland 1987 und in der ehemaligen DDR 1981 stattfand.

Der Zensus 2011 erhebt Basisdaten zu Bevölkerung, Erwerbstätigkeit und Wohnsituation in Deutschland. Die Daten werden ausgewertet, um möglichst genaue Angaben zu erhalten, die als Grundlage für das politische Handeln und die Verwaltung von Bund, Ländern und Gemeinden genutzt werden können. Finanzausgleichszahlungen an Städte und Länder werden von der Anzahl der Einwohner dieser Gebiete abhängig gemacht, Planungen für Kindergärten, Straßen, Versorgungsleitungen usw. und auch die Zuschnitte von Wahlkreisen hängen davon ab, wie die Bevölkerung verteilt ist.

Mit dem Zensus 2011 findet ein grundlegender Methodenwechsel im Vergleich zu den bisher in Deutschland durchgeführten Volkszählungen statt. Die traditionelle Vollbefragung der Bevölkerung wird, u. a. aus Akzeptanz- und Kostengründen, durch ein registerbasiertes Verfahren ersetzt.

9.1.5 Audits im Geleitzug: K3 und BALVI

Die Auditverfahren K3 und BALVI sind „Langläufer“ im ULD. Komplexe Sachverhalte und eine angespannte Personalsituation im MLUR haben die Audits lange verzögert. Jetzt befinden sich die Audits jedoch auf einem guten Weg. Der Abschluss beider Verfahren ist für den kommenden Berichtszeitraum geplant.

Um eine zügige Bearbeitung beider Auditverfahren auch bei personellen Engpässen sicherzustellen, haben das Umweltministerium und das ULD die Auditverfahren stark **aufeinander abgestimmt**. Im Auditverfahren K3 werden primär die

sicherheitstechnischen und formalen Anforderungen an die Dokumentation, das Sicherheitskonzept und die Test- und Freigabeverfahren erarbeitet. Im Auditverfahren BALVI konzentriert sich das Umweltministerium auf das Erstellen einer nachvollziehbaren Vertragsstruktur für ein zentral betriebenes Verfahren. Beide Verfahren stellen die Arbeitsergebnisse dem jeweils anderen Auditverfahren zur Verfügung. Durch diese Arbeitsteilung und Wiederverwertung kann für die Auditverfahren jetzt eine zügige Bearbeitung sichergestellt werden.

Was ist zu tun?
Alle Auditbeteiligten müssen sich an die vereinbarten Terminpläne halten, um die gegenseitige Wiederverwendung von Arbeitsergebnissen zu ermöglichen.

9.1.6 Stadt Lübeck

Das ULD hat mit der Hansestadt Lübeck ein Auditverfahren für das neu eingeführte stadtweite Finanzfachverfahren MACH begonnen. Im Kontext des Umstrukturierens der IT und des Fortlaufens der Verfahrenseinführung stellt sich das Audit als sehr ehrgeiziges Vorhaben dar, das spürbar unter Ressourcenmangel leidet.

Mit 210.000 Einwohnern ist die Hansestadt Lübeck die zweitgrößte Stadt Schleswig-Holsteins. Zwei zentrale aktuelle Projekte sind das **Umstellen des IT-Betriebes** von einer dezentralen zu einer zentralen Struktur sowie das Einführen eines neuen stadtweiten Finanzfachverfahrens. Die Ergebnisse beider Projekte fließen in das begonnene Auditverfahren ein. Von Anfang an hatte der bestehende Ressourcenmangel Folgen:

- Die Aufnahme und Analyse des eigentlichen Finanzfachverfahrens konnte bislang nicht erfolgen.
- Bereits das Durchführen der IT-Strukturanalyse bedeutete einen zeitintensiven Kraftakt.

Es zeigt sich, dass der **Zeitpunkt eines Audits** mit Bedacht gewählt werden sollte. Gerade große Infrastruktur- und Einführungsprojekte in der IT benötigen stets eine gewisse Zeit zur Nachbereitung und Vervollständigung der Dokumentation, bis sie zum endgültigen Abschluss kommen können.

Was ist zu tun?
Die Hansestadt Lübeck sollte den begonnenen Auditprozess konsequent fortführen und hinreichend priorisieren.

9.1.7 azv Pinneberg

Das Auditverfahren beim Abwasser-Zweckverband Pinneberg wurde kontinuierlich vorangetrieben und steht kurz vor dem Abschluss.

Der Abwasser-Zweckverband (azv) war durch seine umfangreichen Auditerfahrungen im Bereich der Qualitätsmanagement- und Umweltmanagementsysteme ideal auf das Datenschutz-Behördenaudit vorbereitet (32. TB, Tz. 9.2.2). Die gemeinsame Arbeit am Auditgegenstand, regelmäßige Kontrollen durch den Auditor des ULD und die kontinuierliche Weiterentwicklung führen dazu, dass der Auditgegenstand bereits einen **hohen Reifegrad** erreicht hat. Der azv plant jedoch für das erste Halbjahr 2011 in einzelnen Teilen des Auditgegenstands noch umfangreiche Änderungen, die beim Audit berücksichtigt werden sollen. Das ULD und der azv gehen davon aus, dass das Verfahren in der Jahresmitte 2011 erfolgreich abgeschlossen werden kann.

Was ist zu tun?
Der azv muss die geplanten Änderungen und Ergänzungen umsetzen. Das ULD wird nach den Änderungen die abschließende Auditprüfung durchführen.

9.1.8 Stadt Pinneberg

Bei der Stadt Pinneberg steht die Reauditierung an.

Dem allgemeinen Trend folgend, wurden in den letzten Jahren auch in Pinneberg Server virtualisiert, Arbeitsplätze mit Thin Clients ausgestattet sowie Multifunktionsdrucker aufgestellt. Das 2006 im Audit hervorgehobene „qualitativ hohe Niveau“ der Dokumentation wurde, das ist bereits absehbar, gehalten. Diese **gute Dokumentation**, die sich auch auf die Dienstvereinbarungen erstreckt, machte sich nach Bekunden des leitenden IT-Planers bei der technischen, organisatorischen und betriebswirtschaftlichen Planung und Durchführung der Umstellungen bezahlt.

9.1.9 Dataport: ISMS für das DCS

Das ULD hat Dataport für das Konzept eines Informationssicherheitsmanagementsystems (ISMS) für das Data Center Steuern (DCS) ein Auditsiegel verliehen.

Das Data Center Steuern ist das gemeinsame Steuerrechenzentrum von Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein. Hier werden die Daten von rund 13.000 Arbeitsplätzen in den 58 Finanzämtern der vier Bundesländer verarbeitet und jährlich rund 12 Millionen Steuerbescheide produziert. Als fünftes Trägerland ist noch 2010 **Niedersachsen** dem norddeutschen Steuerverbund beigetreten. Damit kommen ca. 12.500 Arbeitsplätze in 69 Finanzämtern von Niedersachsen hinzu; die Anzahl der im DCS zu erstellenden Steuerbescheide wird sich verdoppeln.

Die Länder Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein haben mit Dataport als Anstalt öffentlichen Rechts Verträge über die Erbringung von IT-Dienstleistungen für die Steuerverwaltung des jeweiligen Landes im Zusammenhang mit dem Betrieb des Data Center Steuern geschlossen. Das Konzept für das ISMS umfasst eine **umfangreiche Generaldokumentation**. In ihr sind alle Vorgaben und Regelungen zum Themenkreis Datenschutz und Datensicherheit für den Betrieb und die Weiterentwicklung des DCS zusammengefasst.

Dataport hat für den sensiblen Bereich der Steuerdatenverarbeitung **spezielle Sicherheitsmaßnahmen** vorgesehen. So sind administrative Änderungen an den Datenverarbeitungssystemen des Data Center Steuern nur über eine hierfür bereitgestellte Administrationsumgebung möglich. Der administrative Zugang zu den einzelnen Komponenten und Programmen des Data Center Steuern wird über Terminalserver kanalisiert, um eine revisionssichere Protokollierung und durchgängige Nachvollziehbarkeit administrativer Tätigkeiten sicherzustellen. Der Zugriff auf die Administrationsumgebung wird durch eine 2-Faktor-Authentifizierung abgesichert. Diese umfasst den username-/passwortgeschützten Anmeldezugriff auf das System und eine hardwarebasierte Lösung („Besitz und Wissen“). Die Administration der Administrationsplattform erfolgt aufseiten Dataports durch eine eigene Organisationseinheit, die keinen administrativen Zugriff auf die Systeme und Verfahren des Data Center Steuern erhält. Dieses soll verhindern, dass die Administratoren der Steuerverfahren sich selbst oder anderen zusätzliche administrative Zugriffsmöglichkeiten unter Umgehung der revisionssicheren Protokollierung ermöglichen können.

Das Datenschutz- und Sicherheitsmanagement orientiert sich an internationalen Standards. Das **ISMS** folgt den Vorgaben des Standards 100-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Auf Ebene der technischen und organisatorischen Maßnahmen gelten die Vorgaben der IT-Grundschutz-Vorgehensweise gemäß Standard 100-2 des BSI und den IT-Grundschutzkatalogen.

Bei der Durchführung des Audits wurden die folgenden Aspekte festgestellt, die im Sinne einer **datenschutzfreundlichen Gestaltung** von Technik und Organisation besonders hervorzuheben sind:

- Das ISMS des Data Center Steuern gewährleistet durch eine dauerhafte Befassung mit den Themenkreisen Datenschutz und Datensicherheit ein hohes Gesamtsicherheitsniveau.
- Das ISMS und die Sicherheitskonzeption bieten den Auftraggebern des Data Center Steuern eine belastbare Grundlage für eine eigene Sicherheitskonzeption und eigene interne sowie externe Prüf- und Auditverfahren.
- Die Datenverarbeitung wird unter den Aspekten der Verfügbarkeit, Vertraulichkeit, Integrität sowie der Ordnungsmäßigkeit in einer geregelten Aufbau- und Ablauforganisation überwacht.
- Die Sicherheitsprozesse sind unter Berücksichtigung eines national anerkannten Sicherheitsstandards gestaltet.

- Sicherheitsrelevante Ereignisse können über das IT-Sicherheitsvorfallmanagement rechtzeitig erkannt werden.
- Die technischen und organisatorischen Abläufe des ISMS sind vollständig und nachvollziehbar beschrieben.

Was ist zu tun?
Dataport muss das hohe Sicherheitsniveau der beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen halten und kontinuierlich verbessern. Die Auftraggeber sollten durch eigene Audit- und Kontrollverfahren in ihrem Zuständigkeitsbereich das bestehende Audit ergänzen, um eine vollständige Abdeckung der gesamten Steuerdatenverarbeitung zu erreichen.

9.2 Datenschutz-Gütesiegel

9.2.1 Abgeschlossene Gütesiegelverfahren

Das ULD konnte 2010 wieder einigen Produkten ein Datenschutz-Gütesiegel verleihen. Fünf Produkte wurden erstmalig zertifiziert. Dreizehn weitere Produkte wurden nach Fristablauf in einem vereinfachten Verfahren rezertifiziert.

Die deutlich angestiegene Anzahl von **Rezertifizierungen** zeigt, dass das Datenschutz-Gütesiegel einen wirklichen Mehrwert für die Hersteller bringt. Es ist zu beobachten, dass Kunden in einigen Branchen, wie etwa dem Behavioural Targeting oder der Datenvernichtung, in der Regel nach dem Datenschutz-Gütesiegel fragen.

Mehr und mehr Hersteller machen auch von einer **Doppelzertifizierung** zusammen mit EuroPriSe (Tz. 9.3) Gebrauch, um so die Datenschutzfreundlichkeit für den europäischen wie für den deutschen Markt zu dokumentieren. Bei der Doppelzertifizierung können sowohl bei den Gutachtern als auch bei uns als Zertifizierungsstelle Synergieeffekte genutzt und damit Kosten gespart werden.

Folgende Produkte wurden **neu zertifiziert**:

- People Attract (Version 2.2.5): Werbewirkungskontrolle mittels videobasierter Blickkontaktmessung und -analyse von der Vis-à-pix GmbH,
- targ.ad (Version 2): Zielgruppenzugehörigkeitsprognose, die es Werbeanbietern und anderen Anbietern ermöglicht, ihre Werbemittel gezielt auszuliefern,
- Erbringung von Postzustelldienstleistungen (Stand: Juni 2010): von TNT Post erbrachte Bestandteile der Prozessschritte Datenmanagement, Produktion/Sortierung, Transport und Zustellung,
- ElsterOnline Client Server Architektur (Stand: Mai 2010): Client/Server-Architektur zum Austausch von steuerrelevanten Daten,
- Akten- und Datenvernichtung (Stand: Oktober 2010): physikalische Datenträgervernichtungsfunktionalitäten der Firma MAMMUT Dokumentenservice GmbH & Co. KG.

Im **Rezertifizierungsverfahren** wurden folgende Produkte in einem vereinfachten Verfahren (27. TB, Tz. 9.1.4) erneut überprüft und zertifiziert:

- Verfahren der Akten- und Datenträgervernichtung (Stand: Dezember 2009): Verfahren zur Vernichtung von Akten und Datenträgern durch die Lutz von Wildenradt GmbH im Auftrag für öffentliche und nicht öffentliche Stellen,
- SQS-Testsuite für SAP HCM (Version 2.0): Beratungsprodukt zur Qualitätssicherung (Test) von SAP HCM-Anwendungssystemen in der Praxis,
- e-pacs Speicherdienst (Version 3.0): elektronische externe Archivierung von Röntgenbildern und anderen patientenbezogenen medizinischen Daten,
- KOMMBOSS (diverse Module, Version 2.9): Unterstützung von Kommunen und öffentlichen Stellen in den Bereichen Personalwesen, Zentrale Verwaltung und Organisation,
- Elefant Profi im Security-Mode (Version 8.01): Verwaltungsprogramm für psychotherapeutische und ärztliche Praxen,
- Verfahren der Vernichtung von Akten und Mikroformen (Stand: Juni 2010): Vernichtung von Akten und Mikroformen gemäß DIN 32 757 Sicherheitsstufe V aus von der AVZ Kunden zur Verfügung gestellten verschlossenen Containern,
- Verfahrensregister (Version 1.0 (2010)): Unterstützung des betrieblichen Datenschutzbeauftragten bei der Erstellung und Verwaltung eines Verfahrensregisters,
- PROSOZ 14plus (Version 5.8.1): Software-unterstützte Bearbeitung der öffentlichen Jugendhilfe in den Bereichen Fallmanagement, Leistungsgewährung und Controlling,
- wunderloop Integrated Targeting Platform (Stand: Juli 2010): Verfahren zur gezielten Ansprache von Internetnutzern im Bereich der Online-Werbung auf Basis deren Nutzerverhaltens unter Zwischenschaltung eines Anonymisierungsdienstes,
- Easybooth Modell 37, Easybooth V3 Modell 36, Minicabine 3 Modell 38 und UPB Modell 3: digitale Fotokabine mit integrierter biometrischer Bildbearbeitung zur Nutzung in Meldebehörden,
- Verfahren der Akten- und Datenträgervernichtung (Stand: September 2010): Verfahren zur Vernichtung von Akten und Datenträgern durch die recall Deutschland GmbH im Auftrag,
- PKV-Datenpool (Version 1.0): Infrastrukturlösung für den gesicherten Austausch von Abrechnungsdaten zwischen Leistungserbringern und Zahlungsstellen im Bereich der Krankenversicherungen,
- Verfahren zur Vernichtung von Datenträgern (Stand: November 2010): Vernichtung von Akten, Datenträgern und Mikrofilmen durch die Firma Reisswolf Akten- und Datenvernichtung GmbH & Co. KG, Hamburg, im Auftrag.

Weitere Informationen für **Hersteller** finden sich im Internet unter:



https://www.datenschutzzentrum.de/guetesiegel/infos_hersteller.htm

Was ist zu tun?
Die Hersteller von Produkten sind auf die Vorzüge des Gütesiegels hinzuweisen. Es erfolgt eine enge Zusammenarbeit mit dem Projekt EuroPriSe, um Synergien zu nutzen und Hersteller zielgerichtet beraten zu können.

9.2.2 Sachverständige

2010 konnte das ULD deutlich mehr Sachverständige für das Gütesiegelverfahren anerkennen als im vorangegangenen Jahr.

Im Rahmen des Gütesiegelverfahrens erfolgt die Begutachtung der zu zertifizierenden Produkte durch beim ULD anerkannte Datenschutzsachverständige. Wer sich anerkennen lassen möchte, kann dieses entweder für den Bereich Recht oder Technik beantragen. Bei entsprechender **Qualifikation** ist eine Doppelzulassung oder die Anerkennung einer ganzen Prüfstelle möglich. Voraussetzungen für eine Anerkennung ist stets neben der Zuverlässigkeit und Unabhängigkeit der Nachweis der erforderlichen Fachkunde. Diese muss sich insbesondere auf den Datenschutzbereich erstrecken und auch jahrelange praktische Erfahrungen beinhalten.

Hinzugekommen als Sachverständige sind 2010:

- Dipl.-Math. Eva Saar, Darmstadt (Technik),
- Dipl.-Inform. Dr. Reinhard Linz, Bonn (Recht/Technik),
- Dr. Flemming Moos, Hamburg (Recht),
- Joerg Heidrich, Hannover (Technik),
- Christian Regnery, Berlin (Recht),
- Thilo Märtin, Nürnberg (Recht),
- Dipl.-Inform. (FH) Thomas Gutte, Wiesbaden (Technik),
- Oliver Gönner, Alfter (Recht),
- Holger Filges, Kalkar (Technik),
- Dr. Jan Koecher, Hamburg (Recht),
- Dipl.-Ing. Doris Schernus, Hamburg (Technik).

Die Prüfstelle „2B Advice", Bonn, ist mit seinem zweiten Leiter Hans Joachim Bickenbach nunmehr für Recht und Technik anerkannt.

Inzwischen sind 44 Einzelsachverständige **registriert**. 20 Sachverständige sind für den Bereich Recht und 18 für den Bereich Technik anerkannt. Sechs Sachver-

ständige haben die Anerkennung für beide Bereiche. Hinzu kommen neun Prüfstellen, von denen eine für Recht, zwei für Technik und sechs für beides bei uns eingetragen sind.

Die Sachverständigen sind verpflichtet, im Abstand von jeweils drei Jahren nach dem Datum der Anerkennung **Nachweise** über den Besuch von Fortbildungen und von Foren zum Erfahrungsaustausch beizubringen. Zahlreiche Sachverständige sind bereits seit mehr als drei Jahren anerkannt und haben die entsprechenden Nachweise vorgelegt. Ende August 2010 fand der jährliche Gutachterworkshop in Kiel statt. 20 Sachverständige diskutierten über aktuelle Erfahrungen mit Neu- und Rezertifizierungen, vorzeitige Rezertifizierungen, Schutzziele als Leitmotiv für die Prüfung, aktuelle Gesetzgebung und Fragen des Marketings.

Weitere Informationen für Sachverständige befinden sich im Internet unter:


https://www.datenschutzzentrum.de/guetesiegel/akkreditierung.htm

Was ist zu tun?
Die Sachverständigen stellen einen wichtigen Faktor dar, um bei Herstellern Interesse für das Gütesiegel zu wecken. Ihr Antrieb, neue Produkte für das Gütesiegelverfahren zu gewinnen, ist daher zu unterstützen.

9.2.3 Kriterienkatalog De-Mail

Im Auftrag des Bundesministeriums des Innern hat das ULD einen Datenschutz-Kriterienkatalog für De-Mail entwickelt. Dabei konnten unsere Erfahrungen mit dem Anforderungskatalog für Datenschutz-Gütesiegel genutzt werden.

Anbieter von De-Mail-Diensten müssen den Nachweis erbringen, dass sie bei Gestaltung und Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllen. Der aktuelle Entwurf eines De-Mail-Gesetzes macht Vorgaben für die datenschutzgerechte Ausgestaltung der De-Mail-Dienste. Diese betreffen u. a. Account-Eröffnung, Postfach- und Versanddienst, Identitätsbestätigungsdienst, Verzeichnisdienst, Dokumentenablage, Auskünfte, Protollierung und Löschung von Daten. Daneben gelten ergänzend die allgemeinen Datenschutzvorgaben

? ***De-Mail***

wurde zunächst unter dem Begriff „Bürgerportale“ entwickelt und soll eine verbindliche Kommunikation über das Internet ermöglichen. Sicherheit, Vertraulichkeit und Nachweisbarkeit sollen gewährleistet sein, sodass insbesondere im Geschäftsverkehr und bei der Kommunikation mit Behörden auf die Schriftlichkeit verzichtet werden kann. Hierbei wird auch auf die Technik der elektronischen Signatur zurückgegriffen.

Identitätsbestätigungsdienste und Verzeichnisdienste sollen das Vertrauen in die Identität des Kommunikationspartners stärken.

Die Nutzung von Pseudonymen soll zulässig sein, deren Aufdeckung unter bestimmten Bedingungen möglich ist.

insbesondere des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes. Die die Gesetze konkretisierenden **Kriterien** wurden mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abgestimmt. Neben den rechtlichen Vorgaben haben diese die technisch-organisatorischen Maßnahmen und die Rechte der Betroffenen im Blick. Für 2011 sind Workshops mit den Anbietern von De-Mail-Diensten geplant, um ihnen die Kriterien näherzubringen.

Was ist zu tun?
Die Diskussion um die De-Mail-Dienste und gegebenenfalls erfolgende Änderungen an dem Entwurf des De-Mail-Gesetzes sind zu beobachten. Die Kriterien sind entsprechend anzupassen.

9.3 EuroPriSe – europäisches Datenschutz-Gütesiegel



Das im Jahr 2009 eingeführte europäische Datenschutz-Gütesiegel EuroPriSe findet europaweit Interesse und positive Resonanz. Die Nachfrage steigt stetig. Das ULD entwickelt diese Initiative federführend weiter und ist als Zertifizierungsstelle aktiv.

Die rasante Entwicklung von Technologien und elektronischen Dienstleistungen vom Smartphone über soziale Netzwerke bis zu elektronischen Ausweisen schafft neue Möglichkeiten, birgt aber ebenso neue und für viele Bürgerinnen und Bürger unüberschaubare Gefahren. Im Dschungel der neuen Technologien und Angebote brauchen diese ebenso wie Unternehmen richtungweisende Hilfestellungen, denen sie guten Gewissens vertrauen können. EuroPriSe stellt ein wirkungsvolles Instrument zur Herstellung von Vertrauen in Informationstechnologien und eine **Messlatte für die Datenschutzfreundlichkeit** von Produkten und Dienstleistungen im privaten und öffentlichen Sektor bereit.



Das europäische Datenschutz-Gütesiegel wird nach einer eingehenden Prüfung an IT-Produkte und IT-Dienstleistungen verliehen, die sich **in puncto Datenschutz vorbildlich** an die Vorgaben des europäischen Datenschutzrechts halten. Für Verbraucherinnen und Verbraucher bietet das EuroPriSe-Siegel eine informative und zuverlässige Orientierungshilfe. Unternehmen und Diensteanbieter können mit dem von einer unabhängigen, kompetenten Stelle verliehenen Siegel ihren Kunden effektiv nachweisen, dass ihre Produkte und Dienstleistungen dem europäischen Datenschutzrecht entsprechen und eine faire und rechtskonforme Datenverarbeitung ermöglichen.

In dem durch die Europäische Kommission **geförderten Projekt European Privacy Seal (EuroPriSe)** wurden die Grundlagen für das europäische Datenschutz-Gütesiegel geschaffen (32. TB, Tz. 8.9). Seitdem wurde das EuroPriSe-Angebot kontinuierlich weiterentwickelt. Schwerpunkte lagen 2010 auf einer verbesserten Kontrolle der verliehenen Siegel durch die Einführung eines verbindlichen Monitorings von IT-basierten Dienstleistungen und auf einer Verbesserung des Rezertifizierungsverfahrens durch eine kontinuierliche Betreuung durch das sogenannte Update-Verfahren (Tz. 9.3.3).

Die **erfreulich hohe Nachfrage** nach EuroPriSe-Zertifizierungen von Unternehmen aus ganz Europa, aber auch den USA und Südamerika zeigt die Anerkennung unserer erarbeiteten datenschutzrechtlichen Grundsätze und Verfahren über die Landesgrenze hinaus. Europäische Datenschutzstandards, bestätigt durch eine unabhängige Zertifizierungsstelle, sind internationales Qualitätsmerkmal und Wettbewerbsfaktor in der globalen Informationsgesellschaft. Die Zertifizierung des E-Mail-Dienstes „Certified Privnote“ der Firma Insophia mit Sitz in Südamerika macht dies anschaulich.

Die Zertifizierungen im Bereich der verhaltensbasierten Werbung (Online Behavioural Advertising, OBA) zeigen, wie Zertifizierungen nachhaltig den internationalen **Markt beeinflussen** können. Das EuroPriSe-Positionspapier zu den sich aus der Umsetzung der Änderungen aus dem Telekom-Reformpaket (Tz. 9.3.1) ergebenden Anforderungen an Anbieter von OBA-Systemen wurde von der Branche aufgegriffen und wird mit Blick auf eine mögliche Selbstregulierung diskutiert.

Das **Europäische Parlament** hat in einer Resolution im Dezember 2010 die Europäische Kommission aufgefordert, in Zusammenhang mit dem Internet und den neuen Technologien ein gemeinschaftliches System zur Kennzeichnung von Internetseiten nach dem Vorbild von EuroPriSe einzuführen, durch das ersichtlich wird, ob auf einer Seite die Datenschutzbestimmungen eingehalten werden.

9.3.1 Zertifizierungskriterien

EuroPriSe bescheinigt die Vereinbarkeit eines IT-Produkts oder einer IT-basierten Dienstleistung mit den Bestimmungen des EU-Datenschutzrechts. Die im Rahmen einer Zertifizierung zu prüfenden Kriterien sind aus den einschlägigen EU-Richtlinien abgeleitet und in einem Anforderungskatalog aufgelistet.

Dieser Katalog benennt neben den Kriterien die Rechtsnormen, aus denen diese jeweils abgeleitet werden. Zudem listet er Fragen auf, die im Hinblick auf ein Kriterium regelmäßig von Relevanz sind. Der Katalog setzt sich aus vier **thematischen Komplexen** zusammen (31. TB, Tz. 9.4.1):

- 1. Komplex: Grundsätzliche Fragestellungen
- 2. Komplex: Rechtmäßigkeit der Datenverarbeitung

- 3. Komplex: Technische und organisatorische Maßnahmen der Datensicherheit
- 4. Komplex: Betroffenenrechte

Der englischsprachige Anforderungskatalog liegt gegenwärtig in der Version vom November 2010 vor und kann im Internet abgerufen werden unter:


https://www.european-privacy-seal.eu/criteria/

2010 wurde der Anforderungskatalog an die durch das **Telekom-Reformpaket der EU** erfolgten Änderungen der Datenschutzrichtlinie für elektronische Kommunikation angepasst. Das Ende 2009 verabschiedete Reformpaket, das umfassende Änderungen des Rechtsrahmens für Telekommunikationsnetze und -dienste vorsieht, brachte aus Datenschutzsicht die Einführung einer Benachrichtigungspflicht für Telekommunikationsanbieter, falls personenbezogene Daten ihrer Kunden oder anderer Personen kompromittiert werden („security breach notification“), und die Verschärfung der Anforderungen an eine rechtmäßige Verwendung von Browser-Cookies und ähnlichen technischen Hilfsmitteln, die eine Speicherung von Informationen im Endgerät eines Nutzers zur Folge haben.

Dementsprechend ist der EuroPriSe-Anforderungskatalog um zwei neue Kriterien ergänzt worden: Kriterium 2.1.4.1 betrifft das neue Einwilligungserfordernis für die Verwendung von Cookies; Kriterium 4.2.1 setzt das Recht der von einer Kompromittierung personenbezogener Daten betroffenen Personen auf Benachrichtigung durch den betreffenden Telekommunikationsanbieter um.

Der Anforderungskatalog ist darüber hinaus auch um Fragen zur **Sicherheit von Webanwendungen** ergänzt worden, die insoweit typische Themen wie SQL-Injection und Cross-Site Scripting (XSS) betreffen.

Was ist zu tun?
Der Kriterienkatalog ist kontinuierlich weiterzuentwickeln und an Rechtsänderungen sowie alle wesentlichen Neuerungen der Technik anzupassen.

9.3.2 Fachinformationen für EuroPriSe-Gutachter und Antragsteller

Das ULD hat neue Dokumente für EuroPriSe-Gutachter und Antragsteller erstellt, u. a. ein Positionspapier zur Zertifizierbarkeit von Online-Diensten zur Einblendung verhaltensbasierter Werbung und eine Dokumentvorlage zu Anforderungen an die Dokumentation eines Zertifizierungsgegenstands.

Große Nachfrage nach EuroPriSe-Zertifizierungen besteht im Bereich der verhaltensbasierten Werbung im Internet, dem „Behavioural Advertising“. Die Änderung der EU-Datenschutzrichtlinie für elektronische Kommunikation zur Verwendung sogenannter Cookies (Tz. 9.3.1) hat für die EuroPriSe-Zertifizierung von **Online-Behavioural-Advertising-Diensten** Bedeutung, da diese solche Cookies verwenden. Über die Auslegung der neuen Vorschrift besteht allerdings große Rechtsunsicherheit. Deshalb hat das ULD für EuroPriSe in einem umfassenden Positionspapier hierzu Stellung bezogen und die gegenwärtig geltenden

Voraussetzungen für eine Zertifizierung solcher Dienste aufgelistet. Eine deutschsprachige Kurzfassung dieser Stellungnahme ist im Internet abrufbar unter:


https://www.european-privacy-seal.eu/results/fact-sheets/

Ein wichtiger Bestandteil jedes EuroPriSe-Zertifizierungsverfahrens ist die Überprüfung der Dokumentation des jeweiligen IT-Produkts bzw. IT-basierten Dienstes. Dabei geht es z. B. um die Bewertung von Benutzerhandbuch, Datenschutzerklärung, IT-Sicherheitsrichtlinie oder Auftragsdatenverarbeitungsvertrag. Diese erfolgt in erster Linie durch die mit dem jeweiligen Verfahren befassten EuroPriSe-Gutachter. Um diesen eine Hilfestellung für ihre Prüfungstätigkeit zu geben, wurde eine Vorlage zu den **Anforderungen an die Dokumentation** eines IT-Produkts bzw. IT-basierten Dienstes erstellt. Darin werden grundlegende Hinweise zur Überprüfung der Dokumentation gegeben und alle Dokumente aufgelistet, deren Bewertung im Rahmen eines EuroPriSe-Verfahrens obligatorisch ist.

9.3.3 Zertifizierungsverfahren

Das EuroPriSe-Zertifizierungsverfahren besteht aus **zwei Abschnitten** (31. TB, Tz. 9.4.2): Zunächst wird das IT-Produkt oder die IT-basierte Dienstleistung von akkreditierten Sachverständigen evaluiert. In einem zweiten Schritt überprüft eine unabhängige Zertifizierungsstelle das von den Sachverständigen eingereichte Gutachten auf Vollständigkeit und Nachvollziehbarkeit. Sind alle Zertifizierungskriterien erfüllt, verleiht die Zertifizierungsstelle das EuroPriSe-Zertifikat. Dieses ist zwei Jahre lang gültig. Nach Ablauf dieser Zeitspanne oder bei wesentlichen Änderungen kann ein vereinfachtes Rezertifizierungsverfahren durchgeführt werden.

IT-basierte Dienstleistungen und insbesondere webbasierte Dienste werden oft in kurzen zeitlichen Intervallen geändert, ohne dass dies für die Nutzer transparent ist. Deshalb ist bei EuroPriSe das sogenannte **Monitoring** eingeführt worden: Wurde ein IT-basierter Dienst zertifiziert, so muss er während der zweijährigen Gültigkeitsdauer des Siegels von den in das Verfahren involvierten Gutachtern auf seine fortwährende Vereinbarkeit mit den Zertifizierungskriterien überprüft werden. Aufgabe der Gutachter ist es zu verfolgen, ob datenschutzrelevante Änderungen an dem jeweiligen Dienst vorgenommen werden, und – falls ja – zu prüfen, ob der Dienst trotz der Änderungen noch alle anwendbaren EuroPriSe-Kriterien erfüllt. Die Anbieter von IT-basierten Dienstleistungen sind verpflichtet, acht Monate nach der Zertifizierung einen Monitoring Report bei der Zertifizierungsstelle einzureichen, der alle relevanten Änderungen und deren Bewertung beinhaltet. Ein weiterer Bericht ist nach 16 Monaten vorzulegen. Das Monitoring ersetzt jedoch nicht das erfolgreiche Durchlaufen eines Rezertifizierungsverfahrens.

Hersteller bzw. Anbieter können sich nach erfolgter Zertifizierung freiwillig dafür entscheiden, ihr Produkt bzw. ihre Dienstleistung von akkreditierten EuroPriSe-Gutachtern in regelmäßigen Abständen daraufhin überprüfen zu lassen, ob es nach wie vor allen relevanten Zertifizierungskriterien genügt. Werden solche soge-

nannten **Update Checks** durchgeführt, ersetzen diese sowohl das für IT-basierte Dienstleistungen obligatorische Monitoring als auch die Durchführung eines vereinfachten Rezertifizierungsverfahrens. Im Anschluss an die Zertifizierung sind alle sechs Monate von den Gutachtern angefertigte sogenannte Update Check Reports bei der Zertifizierungsstelle einzureichen. Bescheinigen die Gutachter dem IT-Produkt bzw. der -Dienstleistung fortdauernde Compliance mit den EuroPriSe-Zertifizierungskriterien und hat die Zertifizierungsstelle insoweit keine Einwände, so stellt sie nach Überprüfung des letzten, nach 24 Monaten einzureichenden Reports eine Rezertifizierungsurkunde aus. Die Gültigkeit des EuroPriSe-Zertifikats verlängert sich dann um weitere zwei Jahre.

9.3.4 Zulassung von Gutachtern

Als EuroPriSe-Gutachter dürfen nur Datenschutzexperten tätig werden, die das strenge EuroPriSe-Akkreditierungsverfahren erfolgreich durchlaufen haben. Zugelassen sind inzwischen mehr als 110 Sachverständige aus vierzehn Ländern.

Die Evaluierung der zu zertifizierenden IT-Produkte und -Dienstleistungen wird bei EuroPriSe durch akkreditierte Gutachter vorgenommen. Gutachter können für den Bereich Recht und den Bereich Technik akkreditiert werden. Bei Nachweis der nötigen **Fachkunde** ist eine Doppelzulassung als rechtlicher und technischer EuroPriSe-Gutachter möglich.

Seit 2010 können technische und rechtliche Datenschutzexperten, die die für eine Akkreditierung als EuroPriSe-Gutachter erforderliche Berufserfahrung noch nicht in vollem Umfang aufweisen können, aber alle sonstigen Voraussetzungen für eine Zulassung als Gutachter erfüllen, sich als „**EuroPriSe Junior Expert**“ akkreditieren lassen. Junior-Gutachter dürfen EuroPriSe-Evaluierungstätigkeiten durchführen, wenn ein Gutachter sie beaufsichtigt und die Verantwortung für ihre Tätigkeit übernimmt. Durch die Einführung einer Junior-Expert-Akkreditierung erhalten Datenschutzexperten die Möglichkeit, schon zu einem frühen Zeitpunkt ihrer beruflichen Karriere an EuroPriSe-Zertifizierungen mitzuwirken.

Datenschutzexperten mit Interesse an einer Akkreditierung müssen nicht nur ihre Fachkunde und Zuverlässigkeit nachweisen, sondern auch an einem **Ausbildungsworkshop** teilnehmen und ein Trainingsgutachten anfertigen, das den hohen EuroPriSe-Anforderungen entspricht. Im Jahr 2010 wurden in Kiel zwei kostenpflichtige Ausbildungsworkshops durchgeführt. Ingesamt wurden vom ULD bislang sechs Workshops veranstaltet, an denen nahezu 200 Datenschutzexperten aus 14 Ländern teilgenommen haben.

2010 wurden **29 neue EuroPriSe-Gutachter und zwei Junior-Gutachter** akkreditiert. Insgesamt waren zum Ende des Jahres 109 Datenschutzexperten als Gutachter und zwei Datenschutzexperten als Junior-Gutachter zugelassen. 53 Sachverständige sind für den Bereich Recht und 46 für den Bereich Technik akkreditiert, zwölf Sachverständige sind für beide Bereiche anerkannt.

Die Gutachter können für ihre Tätigkeit als Sachverständige mit dem EuroPriSe-Expertenlogo werben.





Die akkreditierten Gutachter kommen aus folgenden **EU-Mitgliedstaaten**: Deutschland (49), Finnland (1), Frankreich (4), Großbritannien (4), Irland (1), Kroatien (2), Niederlande (3), Österreich (13), Schweden (3), Slowakei (1), Spanien (28). Zudem ist auch in Argentinien und den USA jeweils ein Datenschutzexperte als EuroPriSe-Gutachter zugelassen worden.

Anzahl der Gutachter in unterschiedlichen Ländern

Länder	Anzahl Gutachter
Argentina	1
Austria	13
Croatia	2
Finland	1
France	4
Germany	49
Ireland	1
Netherlands	3
Slovakia	1
Spain	28
Sweden	3
UK	4
USA	1

Eine Liste aller zugelassenen EuroPriSe-Gutachter ist abrufbar unter:


https://www.european-privacy-seal.eu/experts/register-experts/

Die Akkreditierung eines Gutachters ist **drei Jahre lang gültig**. Ihre Gültigkeit verlängert sich, wenn der Gutachter aktiv an einem EuroPriSe-Verfahren mitwirkt und ein Langgutachten einreicht oder wenn er an vom ULD angebotenen Fortbildungsveranstaltungen in Gestalt von Workshops („Privacy Trainings“) oder Webinars teilnimmt. In einem Infoblatt werden die Voraussetzungen für eine Verlängerung der Akkreditierung explizit aufgelistet.

Was ist zu tun?
Nach wie vor besteht bei Datenschutzexperten großes Interesse an einer Akkreditierung als EuroPriSe-Experte. Das ULD wird 2011 weitere Ausbildungsworkshops für Gutachter anbieten.

9.3.5 Abgeschlossene und laufende EuroPriSe-Verfahren

Eine größere Zahl von Erst- und Rezertifizierungsverfahren sind derzeit im Gange. 2010 konnten drei Erstzertifizierungen erfolgreich abgeschlossen werden.

Folgende IT-Produkte und -Dienstleistungen wurden **neu zertifiziert**:

- **VALid-POS® Standard Edition** (Version 2): Bei der mit dem EuroPriSe-Siegel ausgezeichneten Software VALid-POS handelt es sich um eine datensparsame Lösung zur Betrugsbekämpfung beim Vor-Ort-Einsatz von EC- und Kreditkarten an Geldautomaten und Kassenterminals, wie sie z. B. in Supermärkten, Einzelhandelsgeschäften und Restaurants zum Einsatz kommen. Mit der Hilfe von VALid-POS kann festgestellt werden, ob sich ein zuvor registriertes Mobiltelefon des Karteninhabers in der Nähe des Geldautomaten oder Kartenterminals befindet, an dem die Karte eingesetzt wird. Ist dies der Fall, so ist es wahrscheinlich, dass die betreffende Karte von der hierzu berechtigten Person und nicht von einem in betrügerischer Absicht handelnden Dritten eingesetzt wird. Mit dem Einsatz von VALid-POS reduziert sich folglich das Risiko dafür, dass eine per Karte initiierte Transaktion aufgrund bankeigener Risikobewertungssysteme fälschlicherweise als verdächtig eingestuft und deshalb verweigert wird.
- **SpeechMagic™ Solution Builder** (Version 2.0): SpeechMagic™ Solution Builder ist eine Workflow-Lösung, die das digitale Diktieren und die Spracherkennung in einer medizinischen Umgebung unterstützt und in ein Krankenhausinformationssystem (KIS) integriert werden kann. Die Software nimmt die Diktate von Ärzten auf und leitet sie an eine Spracherkennungssoftware oder an einen Schreibdienst zur manuellen Transkription weiter. In ihrer schriftlichen Form können die Dokumente der Patientenakte im Krankenhausinformationssystem hinzugefügt werden. SpeechMagic™ Solution Builder unterstützt externe Workflows, bei denen Krankenhäuser mit Heimbüros oder den Anbietern von Transkriptionsdiensten zusammenarbeiten. Zu diesem Zweck ermöglicht die Workflow-Lösung die Pseudonymisierung von Audiodateien und Transkriptionen.
- **Certified Privnote** (Stand: September 2010): Certified Privnote ist ein webbasierter Dienst, der seinen Nutzern den einfachen Austausch verschlüsselter Nachrichten über das Internet ermöglicht. Unter https://certified.privnote.com wird der Dienst angeboten und kann registrierungsfrei genutzt werden: Der Nutzer gibt die auszutauschende Nachricht in ein Texteingabefeld ein und schließt die Nachrichtenerstellung durch einen Klick auf den Bestätigungsbutton ab. Daraufhin wird die Nachricht sowohl im Browser des Nutzers als auch auf dem Certified-Privnote-Server verschlüsselt und dann dort abge-

legt. Der Nutzer erhält eine aus den beiden Zufallsschlüsseln generierte Internetadresse (URL). Diese Adresse übermittelt er über einen beliebigen Kommunikationskanal wie z. B. Telefon oder SMS an den gewünschten Adressaten der Nachricht. Der Empfänger fügt die URL in die Adresszeile seines Browsers ein und kann so die verschlüsselte Nachricht abrufen, entschlüsseln und lesen. Die Nachricht wird nach ihrem (erstmaligen) Abruf vom Server gelöscht.

Die öffentlichen **Kurzgutachten** zu allen verliehenen EuroPriSe-Gütesiegeln sind in englischer Sprache im Internet abrufbar unter:


https://www.european-privacy-seal.eu/awarded-seals/

Ende 2010 gab es mehr als 25 laufende Erst- und Rezertifizierungsverfahren nach EuroPriSe. Bei den Zertifizierungsgegenständen handelt es sich überwiegend um **IT-basierte Dienste**, aber auch um IT-Produkte, insbesondere Software. Sie sind für unterschiedliche Einsatzbereiche bestimmt, etwa für den Gesundheits-, den Finanz- oder den Werbesektor. Viele Zertifizierungsgegenstände sind dem Umfeld des Web 2.0 zuzuordnen.

Nicht nur private Unternehmen, sondern auch **öffentliche Stellen** zeigen Interesse an einer Zertifizierung nach EuroPriSe. In einigen Fällen zählt eine Zertifizierung bereits zu den Vergabekriterien für Aufträge öffentlicher Stellen.

9.3.6 Fachinformationen

Mit Fachinformationen richtet sich EuroPriSe an interessierte Bürgerinnen und Bürger zu spezifischen Fragestellungen.

Auf der Basis der Erfahrung mit den EuroPriSe-Zertifizierungen erarbeitet das ULD zu neuen technischen Entwicklungen in allgemein verständlicher Form Informationsblätter. Solche „**Fact Sheets**“ wurden zunächst zu den Themen verhaltensbasierte Online-Werbung, altersgerechte Assistenzsysteme und Datenschutz-Schutzziele veröffentlicht. Die Fachblätter sind in englischer und deutscher Sprache im Internet abrufbar unter:


https://www.european-privacy-seal.eu/about-privacy

Das **EuroPriSe Privacy Training** wurde als Workshop erstmals 2010 für EuroPriSe-Gutachter und andere Interessierte angeboten. Dabei wurden aktuelle Themen wie Cloud Computing, das Telekom-Reformpaket, Auftragsdatenverarbeitung und spezifische Neuerungen bei EuroPriSe in einem Kreis internationaler Teilnehmer vorgestellt und diskutiert. EuroPriSe-Gutachtern ermöglicht die Teilnahme am Workshop die Verlängerung ihrer Akkreditierung.


https://www.european-privacy-seal.eu/experts/expert-training/index.html

9.3.7 Zusammenarbeit mit anderen Datenschutzbehörden

EuroPriSe strebt die Einbindung weiterer europäischer Datenschutzbehörden in die aktive Zertifizierungsarbeit an.

Dazu wurde ein Trainingsworkshop mit einer nationalen Datenschutzbehörde durchgeführt. In einigen Ländern steht eine fehlende explizite gesetzliche Erlaubnis einer aktiven Einbindung der Datenschutzbehörden als Zertifizierungsstellen entgegen. Auch auf europäischer Ebene wäre eine ausdrückliche Nennung der Aufgabe, freiwillige Prüfungen durchzuführen, förderlich. Wir haben die Europäische Kommission darauf hingewiesen, dass eine solche Regelung im Rahmen der derzeit erfolgenden Überarbeitung der **Europäischen Datenschutzrichtlinie** geschaffen werden könnte.

EuroPriSe ist von Anbeginn als Basis für eine „**Baukastenzertifizierung**“ und als Initiative europäischer Datenschutzbehörden konzipiert. Die Überprüfung eines Produktes oder einer Dienstleistung auf der Grundlage der harmonisierenden EU-Regelungen durch eine unabhängige Datenschutzbehörde sichert weitgehend auch die Vereinbarkeit mit nationalem Datenschutzrecht, das insbesondere in sektorspezifischen Bereichen wie z. B. dem Schul- oder dem Medizinrecht ergänzende Regelungen vorsehen kann. Eine auf EuroPriSe aufbauende Zertifizierung mit nationalen Siegeln, wie z. B. dem schleswig-holsteinischen Gütesiegel (Tz. 9.2), kann als sogenanntes Add-on ohne großen Mehraufwand realisiert werden. Da EuroPriSe als Vorbild für andere nationale Zertifizierungssysteme z. B. in Frankreich (32. TB, Tz. 9.4.6) und aktuell in Spanien dient, sind weitere Synergien zu erwarten.

Was ist zu tun?
Die Kooperation mit den Institutionen der EU und den Datenschutzbehörden in Europa ist fortzusetzen und weiter zu intensivieren.

9.4 D21-Initiative Gütesiegel-Board

Das ULD unterstützt im D21-Gütesiegel-Board die Erarbeitung von Qualitätskriterien für kommerzielle Internetangebote und deren Überprüfung durch private Zertifizierungsstellen.

Die Initiative D21 ist eine Partnerschaft aus Politik und Wirtschaft zur Gestaltung der Informationsgesellschaft. In dem 1999 gegründeten branchenübergreifenden Netzwerk von privaten Mitgliedsunternehmen und Partnern aus dem öffentlichen Bereich in Bund, Ländern und Kommunen besteht seit mehreren Jahren ein Gütesiegel-Board. Dessen Ziel ist es, durch transparente Qualitätskriterien für Internetangebote das Vertrauen für geprüfte E-Commerce-Seiten zu verbessern. Diese **Qualitätskriterien des Verbraucherschutzes** schließen den Datenschutz mit ein. Die Einhaltung der Kriterien bei Webshopanbietern wird durch vier Unternehmen zertifiziert, die Mitglied im Board sind. Am Board sind u. a. auch das Bundesverbraucherministerium und die Verbraucherzentrale Bundesverband beteiligt.

Das ULD wurde als Datenschutzbehörde mit eigenen Zertifizierungserfahrungen eingeladen, im Board mitzuarbeiten.

Das Gütesiegel-Board erfüllt verschiedene Aufgaben: Im Vordergrund steht der Erfahrungsaustausch und die **Weiterentwicklung der Qualitätskriterien** für Webshops. Es ist Beschwerdestelle bei Beschwerden über durch die Gütesiegel-anbieter zertifizierte Shopbetreiber. Daneben geht es um die Koordination und Durchführung von Projekten, Veranstaltungen und Kampagnen zur Förderung von Internetgütesiegeln und die Stellungnahme zu politischen Initiativen wie z. B. zur von der Bundesregierung geplanten Stiftung Datenschutz.

Das ULD trägt mit seinem Expertenwissen zur Verbreitung des Datenschutzes bei **E-Commerce-Angeboten** bei, etwa beim Einsatz von Analysewerkzeugen der Shopanbieter oder bei der Auswertung der Profile von Internetnutzern für Werbezwecke.

Was ist zu tun?
Das Gütesiegel-Board sollte den Gedanken des Verbraucher- und Datenschutzes und den der Zertifizierung bei Angeboten im Internet weiterentwickeln und praktisch begleiten.

10 Aus dem IT-Labor

10.1 Google Analytics

Nach anhaltenden Beschwerden über das Tracking-System „Google Analytics“ hatte Google im März 2010 „die Entwicklung eines globalen browserbasierten Plug-ins“ angekündigt. Das Ergebnis bleibt ungenügend.

Im Mai 2010 war es so weit: Google hob das „**Deaktivierungs-Add-on für Browser** von Google Analytics (BETA)“ aus der Taufe. Nutzer können sich diese Browsererweiterung herunterladen, die automatisch und ohne weitere Konfiguration eine Datenübermittlung an den Tracking-Dienst unterbindet. Die von Google präsentierte Lösung stellt sich bei näherer Betrachtung allerdings als höchstens halbherzig heraus.

> **?** ***Funktionsweise von Google Analytics***
>
> *Webseitenbetreiber können den Programmcode von Google Analytics einfach in ihre Webseite integrieren. Wird die Seite aufgerufen, wird der Browser des Besuchers von der Seite angewiesen, zusätzlich ein Programm, ein sogenanntes Script, vom Google-Server herunterzuladen und auszuführen. Dieses Programm führt auf dem Rechner des Nutzers eine kurze Analyse durch und schickt die gewonnenen Informationen an Google zurück.*

Google beschränkt seine Erweiterung auf die Browser Firefox, Chrome und Internet Explorer. Damit ist zwar der größte Teil des Marktes abgedeckt. Wenig verbreitete Browser wie Opera oder Safari werden jedoch ausgespart, ebenso die Vielzahl mobiler **Browser auf Smartphones**.

Die Installation der Erweiterung gestaltet sich einfach – ohne Einstellungen oder Aktivierungen. Einmal installiert, verhindert die Erweiterung, dass das Analytics-Script Daten an Google sendet. Ärgerlich ist, dass das Script selbst von Googles Servern heruntergeladen wird, sodass doch zumindest die Information, dass eine Seite besucht wurde, an Google übermittelt wird. Die aufmerksame Lektüre der Download-Seite der Erweiterung macht klar, wie feinsinnig Google seine Form von „Opt-Out“ definiert. Es geht nicht um ein Opt-Out aus Google Analytics. Das würde schlicht durch ein Blockieren des Script-Downloads möglich sein. Vielmehr teilt Google artig mit, die Erweiterung teile „dem JavaScript (ga.js) von Google Analytics mit, dass **keine Informationen über den Website-Besuch** an Google Analytics übermittelt werden sollen“.

Ärgerlich ist weiterhin der Umstand, dass die Browsererweiterung nur das Script „ga.js“ behandelt. Google nutzt mit Analytics ein zweites, älteres Script namens „urchin.js“. Webangebote, die dieses Script auf ihren Seiten einbinden, senden fleißig weiter Daten an Google – egal ob der Nutzer die Opt-Out-Erweiterung installiert hat oder nicht. Google sollte die Funktionsweise der Erweiterung überdenken. Die Filterung muss auf **alle Analytics-Scripte** ausgedehnt werden. Nutzer sollten auf die Google-Erweiterungen verzichten und stattdessen in ihrem Browser den Zugriff auf die Analytics-Scripte mithilfe bewährter Filtererweiterungen einrichten. Das ULD gibt hierzu Hilfestellungen.

 https://www.datenschutzzentrum.de/tracking/

Für die Google Analytics nutzenden Webseitenanbieter sind die Änderungen ohnehin keine Lösungen, da das Opt-Out nicht den Anforderungen des **Telemediengesetzes** genügt. Es gilt also weiterhin die Aussage, dass die Nutzung dieses Analysewerkzeugs unzulässig ist.

Was ist zu tun?
Googles Opt-Out-Lösung ist inkonsequent und technisch mangelhaft. Nutzer, die ein Tracking ihrer Internetaktivitäten vermeiden wollen, sollten ihren Browser entsprechend einrichten. Webseitenanbieter sollten weiterhin die Finger von Google Analytics lassen.

10.2 Doodle

Doodle ist ein in der Schweiz beheimateter Online-Dienst, der Terminabsprachen und -organisation vereinfachen soll. Leider gibt es Datenschutzprobleme.

Mit dem Dienst lassen sich ohne Anmeldung Einladungen erstellen, in denen Terminvorschläge enthalten sind. Der Link zu dieser Einladung wird dann allen potenziellen Teilnehmern geschickt. Auf der hinter dem Link stehenden Webseite können die Teilnehmer ihre Terminpräferenzen angeben und bei Bedarf Kommentare hinterlassen. Auf diese Weise lassen sich sehr einfach **Termine abstimmen** – auch in größeren Gruppen. So gut die Idee zunächst klingt, so hat die Umsetzung trotzdem einige Haken.

Der Dienst verwendet das Werbenetzwerk Google AdSense zur Einblendung von Werbebannern. Google Analytics kommt für statistische Auswertungen zum Einsatz (Tz. 10.1). Nutzer von doodle.com müssen also davon ausgehen, dass Informationen über sie **ungefragt in die USA** gesandt werden. Immerhin wendet doodle dabei die von Google angebotene IP-Kürzung an und deklariert die Nutzung von Analytics in der Datenschutzerklärung. Neben dem gratis verfügbaren Basisdienst wird eine werbefreie Premiumvariante angeboten. Nach Auskunft der Betreiber werden dabei aber dieselben Daten an Google übermittelt, sodass ein Premiumkonto in Sachen Datenschutz keinen Mehrwert bietet.

Das Anlegen von doodle-Umfragen ist einfach und für jedermann ohne weitere Registrierung möglich. Ob und welche personenbezogenen Daten dort eingetragen werden, steht im Ermessen der Nutzer. Wer die in den Umfragen eingetragenen Informationen einsehen kann, ist nicht vollständig steuerbar. Da der Zugriff auf eine eingerichtete Umfrage durch Weitergabe des zugehörigen Links erfolgt, besteht **kein effektiver Zugriffsschutz**.

Doodle unternimmt Anstrengungen, damit der Link nicht erraten werden kann. Trotzdem kommen zwangsläufig **unbeteiligte Dritte** in den Besitz der URL, zuvorderst Router- und Zugangsprovider sowie WLAN-Nutzer, die mit dem doodle-Kunden dasselbe Funknetz teilen, beispielsweise im Internetcafé. Aber

auch andere Nutzer des lokalen PCs können über den Browserverlauf sehr einfach die bereits aufgerufenen Umfragen öffnen. Dies ist ein konzeptionelles Problem, das doodle auf seiner Webseite leider verschweigt. Nutzer sollten sich im Klaren sein, dass personenbezogene Daten wie Telefonnummern, Adressen oder persönliche Kommentare unter Umständen in die Hände Unbeteiligter geraten können.

Was ist zu tun?
Nutzer sind von doodle aufzuklären, dass es keinen effektiven Zugriffsschutz auf Umfragen gibt. Die Übermittlung von Daten an Google muss – wenn man doodle nutzen möchte – hingenommen oder durch entsprechende Selbstschutzmaßnahmen unterbunden werden.

10.3 Mobile Endgeräte

Komplexe mobile Endgeräte, sogenannte Smartphones, erfreuen sich zunehmender Beliebtheit und Marktdurchdringung. Mit deren Funktionsvielfalt wächst auch die Zahl der Fragen nach Datensicherheit und dem Schutz personenbezogener Informationen.

Smartphones erlauben den Zugriff auf das World Wide Web, E-Mail und andere Dienste des Internets, enthalten Kameras, Navigationssignalempfänger und unzählige andere Sensoren. Die Telefoniefunktion rückt in den Hintergrund; die mobile Datenverarbeitung rückt nach vorn. Die verschiedenen am Markt vertretenen Smartphone-Angebote lassen sich kaum nutzen, ohne **persönliche Daten** preiszugeben.

Die Apple-Produkte lassen sich nur in Betrieb nehmen, wenn man einwilligt, personenbezogene Daten an Apple zu übermitteln. Bei anderen Anbietern sieht es ähnlich aus. Nutzt man ein Telefon mit dem sich derzeit schnell verbreitenden Linux-Derivat Android, kommt man kaum umhin, sich ein Benutzerkonto bei Google anzulegen. In beiden Fällen werden personenbezogene Daten in die USA übermittelt. Theoretisch könnte man bei Android die Google-Verdrahtung loswerden. Aufgrund seines **Open-Source-Charakters** ist es möglich, das System nach eigenen Wünschen anzupassen. Doch versuchen die meisten Hersteller, ein Einspielen modifizierter Versionen des Betriebssystems auf die Geräte mit technischen Mitteln zu verhindern. Dies wird insbesondere zum Problem, wenn in einer bestimmten Systemversion Sicherheitsmängel entdeckt werden. Bei älteren Geräten lohnt es sich für die Hersteller anscheinend wirtschaftlich nicht mehr, ihre Produkte zu pflegen und Aktualisierungen anzubieten. Findet man im Netz von der Open-Source-Community erstellte Updates für so ein Gerät, kann man sie nicht einspielen, ohne zunächst den Herstellerschutz zu durchbrechen. Letzteres ist dabei rechtlich nicht unproblematisch.

Im Fokus der Datenschützer stehen weiterhin die **Anwendungen**: Bei der Installation bekommt man zwar meist mitgeteilt, auf welche Funktionen des Gerätes ein Programm zugreifen will. Doch lassen sich die Berechtigungen nicht einzeln selektieren. Man kann so nicht steuern, dass ein Programm beispielsweise vom Zugriff auf Netzwerkverbindungen ausgeschlossen ist, wenn man es nicht dafür

verwenden will. Die von Anwendungen ausgehenden Risiken lassen sich so durch die Nutzer nicht einschränken.

Dazu kommt, dass viele Anwendungen fleißig **Daten über die Nutzer sammeln** und an Server im Netz übertragen. Nutzt man alle Möglichkeiten eines Smartphones, ist man nicht der Einzige, der Nutzen daraus zieht. Werden etwa GPS und WLAN aktiviert, werden häufig die eigenen Positionsdaten sowie die gefundener WLAN-Access Points an Navigationsdienstleister übertragen, die damit die Ergebnisse ihrer Dienste verbessern wollen. Positions- und Verhaltensmuster der Anwender sind insbesondere für Werbedienste interessant, die auf die Vorlieben der Nutzer zugeschnittene Anzeigen ausliefern wollen. Nur selten wird für solche Auswertungen ein explizites Einverständnis eingeholt.

Was ist zu tun?
Smartphones müssen sich auch aktivieren und nutzen lassen, ohne dass personenbezogene Daten an die Hersteller übermittelt werden.

Hersteller von Smartphones und Applikationen müssen die Sicherheitskonzepte für ihre Architekturen offenlegen und auf gefundene Fehler schnell mit Updates reagieren.

Nutzer müssen die Möglichkeit haben, installierten Anwendungen die Zugriffsrechte auf Netzwerk, Kamera usw. auch einzeln zuzuweisen oder zu entziehen.

Werden Smartphones von Behörden und Unternehmen eingesetzt, so müssen für die Datenspeicherung auf dem Gerät und die Datenübertragung per Netz offengelegte und von unabhängigen Stellen als sicher anerkannte (Ende-zu-Ende-) Verschlüsselungsmechanismen genutzt werden. Ein Zugriff von Herstellern, Diensteanbietern und Netzbetreibern auf die Daten ist auszuschließen.

10.4 Faxgeräte

Faxgeräte gelten aus technischer Sicht mit ihrer Punkt-zu-Punkt-Verbindung als hinreichend sicher. Für eine sichere Übertragung personenbezogener Daten sind jedoch zusätzliche organisatorische Maßnahmen notwendig.

Wie jedes andere technische Gerät ist das Faxgerät – damit ist zunächst das „einfache“ Stand-alone-Gerät gemeint – bei dem Einsatz in einer Behörde oder einem Unternehmen **bestimmten Gefährdungen** ausgesetzt, z. B.:

- Unbefugte Personen können, wenn sie Zugang zu dem Faxgerät haben, Faxe versenden. Damit erscheint auf der Empfängerseite die Faxnummer des Senders, obwohl das Fax durch eine unberechtigte Person versendet wurde (unbefugte Benutzung von Faxgeräten).
- Unbefugte Personen können, wenn sie Zugang zu dem Faxgerät haben, Faxe mit einer gefälschten abgehenden Nummer versenden. Die abgehende Nummer kann ähnlich wie eine MAC-Adresse gefälscht werden (gefälschte Faxsendungen).

- Personen können, wenn sie Zugang zu dem Faxgerät haben, die Kurzwahltasten eines Faxgerätes umprogrammieren. Damit werden alle Faxe, die mit diesen Kurzwahltasten versendet werden, den falschen Empfängern zugestellt (versehentliches oder vorsätzliches Umprogrammieren der Kurzwahlnummern).
- Unbefugte Personen können, wenn sie Zugang zu einem Faxgerät in einem öffentlichen Bereich haben, Faxsendungen zur Kenntnis nehmen, die nicht für sie bestimmt sind (unbefugtes Lesen von Faxsendungen).
- Unbefugte Personen können Kenntnis von Restinformationen auf Verbrauchsmaterial von Faxgeräten erhalten. Bei Faxgeräten mit Thermotransferfolie werden eingehende Faxsendungen auf eine Zwischenfolie geschrieben, bevor sie ausgedruckt werden. Diese Folie ist Verbrauchsmaterial und muss ausgetauscht werden. Die Inhalte auf dieser Zwischenfolie können wiederhergestellt und ausgelesen werden (unberechtigtes Auslesen von Restinformationen auf Verbrauchsmaterial).

Beim Einsatz von **Faxservern** bestehen spezifische „organisatorische Gefährdungen“. In Adressbüchern oder Verteilergruppen können falsche bzw. zu viele Empfängeradressen gespeichert werden. Das kann dazu führen, dass Faxsendungen an falsche bzw. an zu viele Empfänger verschickt werden. Wenn der Drucker des Faxservers in einem öffentlichen Bereich steht, können unberechtigte Personen Kenntnisse von den ausgedruckten Faxsendungen erhalten. Auch bei der automatischen Verteilung der Faxsendungen durch den Faxserver an die Empfänger können aufgrund von Zuordnungsfehlern unberechtigte Personen Kenntnis von Faxsendungen erhalten, die nicht für sie bestimmt sind. Als Ergebnis bleibt: Die Faxsendung erreicht nicht den Empfänger, den sie erreichen sollte, und der Sender geht davon aus, dass die Faxsendung fehlerfrei den richtigen Empfänger erreicht hat.

Mit einfachen Maßnahmen können diese organisatorischen Mängel gezielt minimiert werden. Für das Faxgerät sollte ein **Systemverantwortlicher** festgelegt werden, der in Zusammenarbeit mit der Leitung, den Fachbereichs- bzw. Abteilungsleitern, dem behördlichen bzw. betrieblichen Datenschutzbeauftragten und der Administration alle technisch-organisatorischen Fragen regelt und im laufenden Betrieb koordiniert, z. B. Zugang, Zugriff, Faxverteilung, Versorgung mit und Entsorgung von Verbrauchsgütern, Regelungen bei Wartungen.

Weiterhin sollten **Regelungen zur Verwendung** des Faxgerätes getroffen werden, beispielsweise folgende Festlegungen:

- welche Daten mit dem Faxgerät versendet werden dürfen,
- wo das Faxgerät steht und wer wann Zugang zum Faxgerät hat,
- ob ein Faxgerät 24 Stunden an 7 Tagen erreichbar sein muss,
- wie ankommende Faxsendungen verteilt werden,
- dass erwartete Faxsendungen sofort am Faxgerät abgeholt werden,

- wenn das Gerät diese Funktion unterstützt, dass zum Ausdrucken am Gerät zunächst eine PIN-Nummer eingegeben werden muss,
- wie Verbrauchsgüter entsorgt werden,
- wie Wartungspersonal beaufsichtigt wird.

Es kann sinnvoll sein, ein **Faxvorblatt** zu erstellen, das für jede Faxsendung verwendet wird. Dieses Vorblatt enthält Informationen über den Sender, z. B. Faxnummer, Ansprechpartner (Name, Telefonnummer, E-Mail), Anzahl der folgenden Seiten und eventuell eine Unterschrift. Damit kann der Empfänger nachvollziehen, ob die Faxsendung vollständig bei ihm eingegangen ist. Wurde die Faxsendung nicht vollständig oder fehlerhaft empfangen, dann kann sich der Empfänger an den genannten Ansprechpartner wenden.

Um zu kontrollieren, ob die organisatorischen Maßnahmen den gewünschten Sicherheitsgewinn bringen, sollte ein Prozess zur **Protokollierung** und zur regelmäßigen Überprüfung festgelegt werden. So kann festgestellt werden, wann welche Faxsendungen an wen versendet wurden, welche Faxnummern in den Kurzwahltasten hinterlegt sind bzw. welche Faxnummern bei einem Faxserver den verschiedenen Verteilern zugeordnet sind.

Alle getroffenen Maßnahmen sind in der **Sicherheitsdokumentation** entsprechend LDSG und DSVO zu dokumentieren. In einer Dienst- bzw. Betriebsanweisung werden die Mitarbeiter der Behörde bzw. des Unternehmens über die Maßnahmen zum Gebrauch des Faxgerätes informiert. In dieser Anweisung sollten auch praktische Hinweise (Was mache ich, wenn …?) zum Faxversand und -empfang aufgenommen werden, beispielsweise:

- Verwenden von Schreddern am Faxgerät, um Faxsendungen mit personenbezogenen Daten datenschutzkonform zu entsorgen.
- Informationen darüber, wann ein Fax verwendet werden darf und wann kein Fax, sondern eine andere Kommunikationsart gewählt werden muss (z. B. bei Daten, die einem besonderen Berufs- und Amtsgeheimnis unterliegen).
- Festlegung, dass Faxsendungen telefonisch angekündigt werden sollen. So kann der Empfänger das Fax am Gerät direkt entgegennehmen und Fehlsendungen werden gleich zur Kenntnis genommen. Auch eine telefonische Rückversicherung, ob der Empfänger eine Faxsendung vollständig und fehlerfrei erhalten hat, ist denkbar.
- Festlegung, dass es bei empfangenen „eigenartigen“ Faxsendungen zu einer telefonischen Rückversicherung kommt, ob eine Faxsendung auch tatsächlich vom Absender abgeschickt wurde. So kann eine Fälschung der Absenderadresse ausgeschlossen werden.
- Verfahren zum Schutz vor Fehlzustellung (und damit einer unbefugten Kenntnisnahme) einer Faxsendung durch Falscheingabe der Faxnummer durch Vertippen: Zunächst wird ein Dummy-Fax (z. B. nur das Deckblatt) an den Empfänger versendet. Bestätigt dieser den erfolgreichen Empfang, kann die eigentliche Faxsendung durch Betätigen der Wahlwiederholung versendet werden. Auch danach kann eine Bestätigung des Empfängers erfolgen.

Immer häufiger wird die Faxfunktion im Zusammenhang mit modernen **Multifunktionsgeräten** angeboten. Bei deren Einsatz sollten zusätzlich zu den hier aufgeführten Maßnahmen die Hinweise in der Veröffentlichung „Sicherheitsmaßnahmen bei modernen Multifunktionsgeräten (Drucker, Kopierer, Scanner, FAX)“ im Internet berücksichtigt werden.


https://www.datenschutzzentrum.de/kopierer/

Was ist zu tun?
Analysieren Sie den Einsatz Ihrer Faxgeräte in Bezug auf Technik und Organisation.

Benennen Sie einen Systemverantwortlichen für das Faxgerät, der alle technisch-organisatorischen Maßnahmen in diesem Zusammenhang koordiniert.

Legen Sie organisatorische Maßnahmen zur Verwendung der Faxfunktion fest und dokumentieren Sie diese in Ihrer Sicherheitsdokumentation.

Erstellen Sie eine Dienst- bzw. Betriebsanweisung für die Mitarbeiter.

Kontrollieren Sie die Einhaltung der getroffenen Sicherheitsmaßnahmen.

11 Europa und Internationales

Das Jahr 2010 brachte auf internationaler Ebene keine erkennbaren Fortschritte für den Datenschutz. Auf der **32. Internationalen Konferenz** der Datenschutzbeauftragten in Jerusalem Ende Oktober fand zwar ein reger Informations- und Meinungsaustausch statt. Bestrebungen in Richtung völkerrechtlicher Absicherung des Datenschutzes sind aber weiterhin nicht in Sicht.

Kurz danach legte die Europäische Kommission ein „Gesamtkonzept für den **Datenschutz in der Europäischen Union**“ vor. Darin bekennt sich die Kommission zu einer grundrechtsorientierten Weiterentwicklung des Datenschutzes in der EU auf allen Ebenen, insbesondere durch eine Fortschreibung der Europäischen Datenschutzrichtlinie von 1995 und durch Einbeziehung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in das allgemeine Datenschutzrecht. Sie sondiert die Einführung europäischer Zertifizierungsregelungen und will sich für die Festlegung hoher rechtlicher und technischer Datenschutzstandards auf internationaler Ebene einsetzen.



http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:DE:HTML

11.1 Safe Harbor weiter in der Kritik

Das Safe-Harbor-Abkommen, das für Wirtschaftsunternehmen einen vereinfachten Datenaustausch zwischen der Europäischen Union und den USA eröffnet, steht weiterhin unter Beschuss.

Die Kritik des ULD an Safe Harbor (32. TB, Tz. 11.4) wird vom Zusammenschluss der deutschen Datenschutzaufsichtsbehörden, dem Düsseldorfer Kreis, geteilt. Dieser beschloss, dass **in die USA Daten exportierende Unternehmen** die über Safe Harbor erfolgte Selbstzertifizierung jeweils überprüfen müssen. Die im Internet hierzu verfügbaren Informationen sind häufig falsch und inaktuell und entsprechen oft nicht den rechtlichen Anforderungen.



https://www.datenschutzzentrum.de/internationaler-datenverkehr/Beschluss_28_29_04_10neu.pdf

Ein Austausch mit einer australischen Forschungseinrichtung ergab, dass sich gegenüber einer Untersuchung im Jahr 2008 keine praktischen Verbesserungen ergeben haben. Danach behaupten 2.170 US-Unternehmen, gemäß Safe Harbor privilegiert zu sein, wovon aber 388 beim US-Handelsministerium überhaupt nicht registriert waren. Von den dort aufgeführten Unternehmen waren 181 Zertifikate schon wegen ihres Zeitablaufs nicht mehr gültig. Bei Überprüfung allein des Safe-Harbor-Grundsatzes der „Durchsetzung“ ergab sich, dass von den 2.170 US-Unternehmen 940 für Betroffene keine Informationen bereitstellen, wie diese ihre Rechte durchsetzen können. Bei 314 weiteren Unternehmen ist ein Verfahren vorgesehen, das die Betroffenen zwischen 2.000 und 4.000 Dollar

kostet. Es ist kein Wunder, dass hier kein einziges Beschwerdeverfahren durchgeführt wurde: Trotz insgesamt jährlich über 2.000 Beschwerden wegen Verletzung der Safe-Harbor-Grundsätze hat die in den USA zuständige Federal Trade Commission (FTC) nur sieben Unternehmen abgemahnt, weil sie sich zu Unrecht auf Safe Harbor berufen haben.

Was ist zu tun?
Das Safe-Harbor-Abkommen sollte von der EU gekündigt werden, damit über Neuverhandlungen eine reale Sicherung des Datenschutzes bei dem Datenaustausch mit den USA erreicht wird.

11.2 Internationale Standardisierung von Datenschutz

„Privacy by Design“ bedeutet, dass Datenschutz bei der Gestaltung von Technik und organisatorischen Abläufen eingeplant und umgesetzt wird. Damit lassen sich datenschutzrechtliche Probleme von vornherein vermeiden. Die internationale Standardisierung von Datenschutz soll an diesem Punkt ansetzen.



Bereits seit 2007 beteiligt sich das ULD an internationaler Datenschutznormung und wirkt in verschiedenen Standardisierungsorganisationen im Rahmen von europäischen Forschungsprojekten mit (32. TB, Tz. 2.3.2). Ein Schwerpunkt besteht in der Mitarbeit in der Arbeitsgruppe zu **Datenschutz und Identitätsmanagement** der Internationalen Standardisierungsorganisation (ISO). Innerhalb dieser Arbeitsgruppe ist es gelungen, andere Datenschutzbehörden enger in die Mitarbeit einzubinden: Seit vergangenem Jahr wirken auch Vertreter der französischen Datenschutzbehörde CNIL direkt an der Arbeit mit; mit der Artikel-29-Datenschutzgruppe, dem Koordinationskreis aller nationalen Datenschutzbehörden in der EU, besteht mittlerweile eine etablierte Zusammenarbeit, die gemeinsam durch die CNIL und das ULD koordiniert wird.

Nach gut drei Jahren stehen die ersten internationalen ISO-Standards zu Datenschutz und Identitätsmanagement vor der Veröffentlichung. Eine Finalisierung des Standards ISO 29100, eines Rahmenstandards zum Datenschutz, zeichnet sich ab. Hiermit werden wohl erstmalig grundlegende Begriffe und Prinzipien des **Datenschutzes weltweit** in einem technischen Standard übergreifend normiert. Zeitgleich entstehen darauf aufbauende spezifische Standards, z. B. ISO 29101 – Privacy Reference Architecture (Datenschutzreferenzarchitektur) und ISO 24760 – A Framework for Identity Management (Rahmen für Identitätsmanagement). Letzterer bildet u. a. eine Basis für datenschutzförderndes Identitätsmanagement.

Es zeigt sich, dass die Abdeckung der **Vielzahl sektorspezifischer Standards** für die Datenschutzbehörden personell nicht zu leisten ist, obwohl diesbezüglich ein hoher Bedarf besteht. Initiativen, die hier nach Lösungen suchen, haben sowohl auf nationaler Ebene innerhalb des DIN e.V. als auch auf der Ebene der ISO im

Rahmen eines eigens eingerichteten Steuerungskomitees („Privacy Steering Committee“) ihre Arbeit aufgenommen.

Neben der ISO haben **weitere Standardisierungsorganisationen** das Potenzial der Datenschutzstandardisierung erkannt. So gibt es u. a. im „Internet Architecture Board“, einer gemeinsamen Struktur des World Wide Web Consortiums (W3C) und der Internet Engineering Task Force (IETF), erste Versuche, dem Datenschutz einen höheren Stellenwert einzuräumen. Auch in diesen Organisationen, die sich durch hohe Relevanz für die Entwicklung von Standards für das Internet auszeichnen, wirkt das ULD gelegentlich mit und lässt eigene Initiativen einfließen. Ergebnisse der Forschungsarbeiten des ULD, die im vergangenen Jahr diskutiert wurden, sind ein Basisterminologiedokument zur Begriffswelt der Datenminimierung und der Vorschlag „Privicons“ zu grafischen Symbolen (Icons), mit deren Hilfe ein Absender einer E-Mail gegenüber den Empfängern den gewünschten Umgang mit der Nachricht in Bezug auf Geheimhaltung, Weitergabe oder Ähnliches ausdrücken kann.

Was ist zu tun?
Internationale Standards bieten ein hohes Potenzial für einen „Datenschutz durch Technik“, der Datenschutzrisiken schon bei der Entwicklung technischer Systeme minimiert. Daher sollten Datenschutzexperten bei der Erarbeitung der Standards mitwirken. Die Arbeit an diesen Standards sollte so organisiert werden, dass eine effektive Beteiligung von Datenschutzexperten trotz knapper personeller Kapazitäten in den Behörden möglich ist.

12 Informationsfreiheit

12.1 Der schwierige Weg zu einem einheitlichen Informationszugangsrecht

Die Vereinbarung im Vertrag der Koalitionsparteien zur Zusammenfassung des Informationsfreiheitsrechts versprach eine schnelle Lösung mit entbürokratisierender Wirkung. Das Ergebnis liegt auf der langen Bank der Bürokratie.

Die **Zusammenfassung** von Umweltinformationsgesetz (UIG) und Informationsfreiheitsgesetz (IFG) zielt auf Verwaltungsvereinfachung ab. Durch einheitliche Verfahren entfallen aufwendige Abgrenzungsprüfungen. Zugleich können Synergien genutzt und den Bürgerinnen und Bürgern eine transparente Vorgehensweise geboten werden. Auf der Basis der Koalitionsvereinbarung formulierte das ULD umgehend einen Gesetzesvorschlag, der im Ergebnis UIG und IFG zusammenführt und Bereinigungen des Verfahrens vornimmt. Statt der 15 Paragrafen des UIG und den 18 des IFG sollte das neue Informationszugangsgesetz (IZG) 19 Paragrafen enthalten, die Doppelungen systematisch vermeiden. Das ULD stellte den Entwurf den Regierungsfraktionen zur Verfügung – eigentlich eine einfache und klare Sache.



Doch dann wurden wir von einem **Kabinettsvorschlag** zur Änderung des UIG überrascht, der eine angeblich nötige Anpassung an Richtlinien der Euroäischen Union (EU) vorsah, ohne die Koalitionsvereinbarung zu berücksichtigen. Nachdem dies erkannt wurde, schmort der eingebrachte Gesetzentwurf unerledigt in den Landtagsausschüssen. Der Entwurf des ULD wurde dem Umweltministerium, von dem die UIG-Änderung stammt, zur Stellungnahme gegeben. Dieses meinte im März 2010 in einem Vermerk, der ULD-Entwurf sei geprägt von unsystematischen, unpraktikablen und zum Teil unscharfen bzw. umgangssprachlichen Regelungen und sei deshalb zu verwerfen. An einer Stelle wird beklagt, der ULD-Entwurf überhöhe den Datenschutz als Schranke zu Unrecht; an anderer Stelle beklagte das Ministerium, der Datenschutz werde in nicht vertretbarem Maße strapaziert. Der Eindruck, dass Ressortdenken vor Sachlichkeit gestellt wurde, war nicht ganz zu vermeiden. Im April 2010 ging das ULD auf diese Kritik im Detail ein und widerlegte jedes der vorgetragenen Argumente gegenüber den Fraktionen.

Was ist zu tun?
Der Landtag sollte sich nicht weiter von Trägern unbegründeter bürokratischer Bedenken bremsen lassen und ein einheitliches Informationszugangsrecht für Schleswig-Holstein auf den Weg bringen.

12.2 Betriebs- und Geschäftsgeheimnisse: Auskunft über Vertragsgestaltungen

Alle Jahre wieder stellt sich die Frage, unter welchen Bedingungen sich Behörden zur Abwehr von Informationsersuchen auf Betriebs- und Geschäftsgeheimnisse berufen können.

Ein Antrag auf Zugang zu Informationen kann abgelehnt werden, wenn durch die Übermittlung der Informationen ein **Betriebs- oder Geschäftsgeheimnis** offenbart würde und die schutzwürdigen Belange des Betroffenen das Offenbarungsinteresse der Allgemeinheit überwiegen. Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Geschäftsgeheimnisse betreffen in erster Linie kaufmännisches Wissen.

Auch **Bieterunterlagen** erfüllen in der Regel die Anforderung an ein Geschäftsgeheimnis. Dies gilt aber nicht für alle Bestandteile eines Angebots oder eines Vertrages. Die Angabe zum Gesamtangebotspreis enthält üblicherweise keine Informationen zur betrieblichen Situation des Bieters, anders als Kostenkalkulationen Aussagen zum Umfang der Beschäftigung von Fremdkräften oder zu den durch die Aufgabenerledigung entstandenen Kosten machen. Wenn Informationen aufgrund von Geschäftsgeheimnissen nicht zugänglich gemacht werden dürfen, besteht jedoch trotzdem ein Anspruch auf Zugang zu den übrigen Informationen. Die generelle Verweigerung des Informationszuganges aufgrund von vorliegenden Betriebs- und Geschäftsgeheimnissen ist nicht zulässig.

Was ist zu tun?
Behörden müssen bei einem Einsichtsersuchen in Verträge prüfen, ob diesem Geschäfts- und Betriebsgeheimnisse entgegenstehen. Dazu gehören in der Regel kalkulatorische Angaben. Die Behörde hat dann einen beschränkten Zugang zu gewähren.

12.3 Keine Informationskosten für nicht rechtsfähige gemeinnützige Vereine

Das Informationsfreiheitsgesetz sieht nicht ausdrücklich eine Antragsberechtigung für nicht rechtsfähige Vereine vor. Da dahinter immer eine natürliche Person steht, ergibt sich kein praktisches Problem – außer bei den Kosten.

Natürliche Personen sind nach dem Informationsfreiheitsgesetz (IFG) gebührenpflichtig. Gemeinnützige rechtsfähige Vereine hingegen sind nach dem Verwaltungskostengesetz (VwKostG SH) generell **von der Gebührenpflicht befreit**. Stellt sich also die Frage, ob nicht rechtsfähige Vereine rechtsfähigen Vereinen

bei der Anwendung des IFG gleichgestellt werden können und müssen. Der Gesetzesbegründung zum IFG lässt sich diesbezüglich nichts entnehmen. Wir halten es jedoch für sachgerecht, nicht rechtsfähige Vereine und rechtsfähige Vereine in Bezug auf die Antragsberechtigung gemäß dem IFG gleichzustellen. Das Bundesverwaltungsgericht hat zum Umweltinformationsgesetz des Bundes festgestellt, dass auch nicht rechtsfähige Vereine einen Anspruch auf Informationszugang haben, soweit der Rechtskreis der Vereinigung durch die konkrete Maßnahme berührt wird und der Verein eine gewisse Kontinuität und ein Mindestmaß an organisatorischer Struktur aufweist. Hinsichtlich des geltend gemachten Rechts muss der nicht rechtsfähige Verein in einem bestimmten Bereich oder in Bezug auf eine bestimmte Angelegenheit nach einem Rechtssatz des materiellen Rechts Rechtssubjekt sein. Dies lässt sich auf unser IFG nach Sinn und Zweck übertragen. Gründe für die Ungleichbehandlung von nicht rechtsfähigen und rechtsfähigen Vereinen sind nicht ersichtlich. Nicht rechtsfähige Vereine, soweit sie organisatorisch hinreichend verfestigt sind, eine gewisse Kontinuität und ein Mindestmaß an organisatorischer Struktur aufweisen, sind daher nicht nur gemäß dem IFG antragsberechtigt. Sie können sich auch nach dem VwKostG SH auf ihre Gebührenbefreiung berufen.

Was ist zu tun?
Generell ist der Antragsteller über die anfallenden Gebühren vor dem Informationszugang zu informieren. Für nicht rechtsfähige Vereine ist eine Gebührenbefreiung im aufgeführten Fall anzunehmen.

12.4 Einzelfälle

12.4.1 Polizeibeamte und tote Hunde – keine Preisgabe der Identität der Beamten

Will ein von einer Polizeimaßnahme Betroffener einen Schaden geltend machen und benötigt er hierfür Informationen, so kann das IFG dienlich sein.

Innerhalb des letzten Jahres kam es auf den Autobahnen A1 und A2 bei Bad Oldesloe zu drei Vorfällen, bei denen Hunde mit Streifenwagen absichtlich überfahren wurden. Die Halterin eines der überfahrenen Hunde begehrte nach dem IFG Informationen zur Identität der an den Polizeieinsätzen beteiligten Beamten. Der Antrag auf Informationszugang ist im Falle der Bekanntgabe personenbezogener Daten abzulehnen, es sei denn, der Antragsteller macht ein **rechtliches Interesse** an der Kenntnis der begehrten Informationen geltend und überwiegende schutzwürdige Belange der Betroffenen stehen dem nicht entgegen.

Das rechtliche Interesse setzt eine konkrete Rechtsbeziehung zwischen Antragsteller und Betroffenem voraus. Von Bedeutung ist etwa, dass der Antragsteller glaubhaft darlegt, mit dem Betroffenen in einer vertraglichen Beziehung zu stehen, oder dass **zivilrechtliche Ansprüche** gegen den Betroffenen verfolgt werden. Ein rechtliches Interesse an der Offenbarung der Daten setzt voraus, dass eine konkrete Rechtsbeziehung zwischen Antragsteller und Betroffenem besteht. Im konkreten Fall lag eine derartige Rechtsbeziehung zu den Beamten als Perso-

nen nicht vor, sondern zur Polizei, für die die Beamten tätig wurden. Die Petentin hatte also keinen Anspruch auf Kenntnis der Identität der Polizeibeamten.

Was ist zu tun?
Besteht ein rechtliches Interesse des Antragstellers, so kann nach dem IFG ein Zugangsersuchen zu dessen Durchsetzung nicht zurückgewiesen werden.

12.4.2 Gefährdungsbeurteilungen

Ein IFG-Antrag kann lediglich auf Zugang zu den vorhandenen Informationen gerichtet sein, unabhängig davon, ob eine Behörde zu einer Beurteilung gesetzlich verpflichtet war.

Eine Petentin forderte Einsicht in eine Dokumentation zur Gefährdungsbeurteilung nach dem Arbeitsschutzgesetz sowie in eine Dokumentation zu den psychischen Belastungen am Arbeitsplatz. Gefährdungsbeurteilungen für Arbeitsplätze können sehr umfangreiche Papiere sein, die von der staatlichen Arbeitsschutzbehörde im Rahmen ihrer Aufsichts- und **Überwachungstätigkeit eingesehen**, aber in den wenigsten Fällen mitgenommen werden. Soweit die staatliche Arbeitsschutzbehörde bei der Unfallkasse Nord die entsprechenden Gefährdungsbeurteilungen nicht kopiert bzw. mitgenommen hat, gelten diese als nicht vorhandene Informationen nach dem IFG.

Was ist zu tun?
Aus dem IFG ergibt sich keine Verpflichtung der Behörden, nicht vorhandene Informationen zu rekonstruieren oder zu beschaffen.

12.5 Agrarsubventionsempfänger im Internet – Ende eines Konfliktes

Mit dem Urteil des Europäischen Gerichtshofes vom November 2010 ist die Auffassung des ULD zur Veröffentlichung personenbezogener Daten von Empfängern von Agrarsubventionen bestätigt und ein langer Konflikt beendet worden.

Seit 2009 veröffentlichten alle EU-Staaten jedes Jahr Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums. Dabei wurden für jeden Begünstigten die Beiträge unter Nennung des Namens und des Wohnortes der Person oder Organisation, welche die Subventionen erhält, genannt. Diese **Veröffentlichungen personenbezogener Daten** wurden vom ULD kritisch gesehen (31. TB, Tz. 12.1; 32. TB, Tz. 12.2). Der Europäische Gerichtshof hat nun nach Vorlage durch ein deutsches Gericht entschieden, dass die Rechtsvorschriften, die eine Veröffentlichung der Namen natürlicher Personen, die Empfänger derartiger Beihilfen sind, vorschreiben, teilweise ungültig sind. Diese Verpflichtung zur Veröffentlichung verletzt das Recht auf den Schutz personenbezogener Daten. Zukünftig dürfen die Empfänger von EU-Agrarsubventionen nicht mehr in der bisherigen Form veröffentlicht werden.

Eine Veröffentlichung zu natürlichen Personen darf lediglich in anonymisierter Form erfolgen.

Was ist zu tun?
Die Veröffentlichung der Daten zu EU-Subventionen sind inzwischen datenschutzkonform gestaltet. An dieser normativ abzusichernden Praxis muss festgehalten werden.

13 DATENSCHUTZAKADEMIE Schleswig-Holstein

Die Fortbildungsangebote der DATENSCHUTZAKADEMIE Schleswig-Holstein bieten qualifizierte und kostengünstig maßgeschneiderte Unterstützung für optimale Datenverarbeitung und IT-Sicherheit in Verwaltung und Betrieben, in sozialen, schulischen und medizinischen Einrichtungen.



Im Schulungsjahr 2010 fanden **27 Kurse** statt, in denen **541** Personen von zwölf Dozentinnen und Dozenten der DATENSCHUTZAKADEMIE in den verschiedensten Bereichen von Datenschutz, Datensicherheit und Informationsfreiheit geschult wurden.

Elf Absolventen des neuen Power-Lehrgangs „Datenschutz & Datensicherheit“ konnten sich nach erfolgreicher theoretischer und praktischer Prüfung als **„Systemadministrator mit Datenschutzzertifikat“** beglückwünschen lassen. Mit dem Erwerb des Zertifikats können sie nachweisen, dass sie Einsatz und Betrieb von IT-Systemen datenschutzrechtlich sicher beherrschen.

NEU * NEU * NEU * NEU

E-Learning

Die positiven Erfahrungen aus dem Power-Lehrgang haben zur Konzeption neuer E-Learning-Kurse geführt. Eine E-Learning-Plattform sowie elektronische und multimediale Schulungsbestandteile ermöglichen berufsbegleitendes, zeit- und ortsunabhängiges Lernen.

(Vgl. die Kurse PL, LINUX und NET im Jahresprogramm 2011.)

NEU * NEU * NEU * NEU

Die Systemadministratoren mit Datenschutzzertifikat können nicht nur ihre persönliche und berufliche Qualifikation verbessern, sie geben auch ihren Arbeitgebern und den Datenschutzbeauftragten die Sicherheit, dass die vorgeschriebenen technischen, organisatorischen und datenschutzrechtlichen Vorschriften bei der Systemadministration berücksichtigt werden.

Im Rahmen der „DATENSCHUTZAKADEMIE vor Ort“ nahmen in 15 Sonderkursen weitere 225 Personen an Fortbildungen zu folgenden Themen teil:

- Grundlagen der IT-Sicherheit
- Einführung in den Sozialdatenschutz
- Einstieg in das Datenschutzrecht
- Der gläserne Beschäftigte
- Datenschutz in der Verkehrsüberwachung
- Das BSI-Grundschutztool
- Datenschutzrecht der Kranken- und Pflegekassen

- Datenschutz für IuK-Administratoren
- Technischer Datenschutz/Systemdatenschutz
- Arbeitnehmerdatenschutz
- Einführung in den BSI-Grundschutz

Diese **Inhouse-Veranstaltungen** wurden in Auftrag gegeben von

- der Technischen Universität Hamburg,
- dem Statistikamt Nord,
- der Landwirtschaftlichen Sozialversicherung,
- dem Jobcenter Kiel,
- dem Kreis Schleswig-Flensburg,
- der Hansestadt Lübeck,
- den Mürwiker Werkstätten,
- dem Hauptpersonalrat des Wirtschaftsministeriums,
- dem Schleswig-Holsteinischen Landtag,
- dem Ministerium für Landwirtschaft,
- der TNG AG,
- dem Allgemeinen Verband der Wirtschaft Norddeutschlands e.V.

Zur **Sommerakademie** der DATENSCHUTZAKADEMIE Schleswig-Holstein konnten 450 Gäste aus allen gesellschaftlichen Bereichen begrüßt werden. Thema der traditionell Ende August stattfindenden Veranstaltung war diesmal „Codex digitalis – Grundrechtsschutz durch künftige Normen und Techniken“. Dabei wurde die Notwendigkeit einer umfassenden Modernisierung des gesamten Datenschutzrechts unter den Bedingungen einer digitalisierten globalen Welt mit unterschiedlichsten Regelungsmechanismen in den Fokus gestellt.

Im vergangenen Jahr waren so durch Angebote der DATENSCHUTZAKADEMIE insgesamt **1.216 Personen** auf ganz unterschiedlichen Ebenen mit Datenschutzfragen befasst.

Als sehr arbeitsintensiv und anspruchsvoll gestaltete sich der neu eingeführte **Power-Lehrgang „Datenschutz & Datensicherheit“**. 20 Teilnehmer trafen sich in acht 7-stündigen Workshops im ULD, um sich ein qualifiziertes Wissen zum technisch-organisatorischen Datenschutz mit dem Schwerpunkt auf Client/Server-Umgebungen unter Windows 2003/2008 zu erwerben. Eine externe Festplatte, auf der sich mehrere Übungsumgebungen (VMware Images von Client/Server-Betriebssystemen) befinden, ging zum Kursende in den Besitz der Teilnehmer über. Im von den Dozenten für die Kursdauer bereitgestellten E-Learning-Forum konnte untereinander diskutiert und Fragen zum Lehrinhalt gestellt werden.

Diese Erfahrungen mit **E-Learning-Methoden** gingen in die Vorbereitungen für neue Kurse in diesem Lernmodus ein, die 2011 erstmals eingeführt werden: „Linux als Serversystem sicher einsetzen“ (LINUX) und „Netzwerksicherheit“ (NET) (vgl. Jahresprogramm 2011, S. 38/39) werden im kommenden Jahr als E-Learning-Veranstaltung mit einem Präsenztermin angeboten werden. Der weitere Arbeitsaufwand von vier bis fünf Tagen pro Kurs kann von den Teilnehmenden zeit- und ortsvariabel erledigt werden.

NEU * NEU * NEU * NEU

Workshop
Datenschutz in Online-Spielen (DOS)

Die Entwicklung und der Betrieb von Online-Spielen für Browser, Konsolen, PCs, Handheld und sozialen Netzwerken wird in diesem Workshop unter Beachtung der Datenschutzvorgaben erarbeitet.

(Vgl. im Jahresprogramm 2011, S. 35.)

NEU * NEU * NEU * NEU

Die bewährten **IT-Sicherheitskurse** (unter Berücksichtigung der BSI-Grundschutztools) werden weiter ausgebaut. Dazu gehören: „IT-Sicherheitsmanagement“ (ITS-I), „Sicherheitsmanagement auf Basis von IT-Grundschutz“ (ITS-II), „Mit dem BSI-Grundschutztool zum IT-Sicherheitskonzept“ (BSI-GST). Die Kurse befähigen die Absolventen, die Sicherheit von Verfahren oder Geschäftsprozessen und die Verwaltung von IT-Verbünden von Organisationen mithilfe der IT-Grundschutzmethode umzusetzen. 2011 wird der neu konzipierte Kurs „BSI IT-Grundschutz, Praktische Umsetzung in einer Organisation“ (BSI-Praxis) dieses Themenspektrum erweitern.



Die seit jeher gut eingeführten und besuchten **Grundlagenkurse** der DATENSCHUTZAKADEMIE werden weiterhin gut angenommen, seien dies „Datenschutzrecht/Datensicherheitsrecht für behördliche Datenschutzbeauftragte“ (DR/DT), „Einführung Datenschutz im Schulsekretariat“ (ES) oder „Führung von Personalakten“ (PA). Im kommenden Jahr wird der Kurs „Rechtsfragen des Landesdatenschutzgesetzes“ (LDSG-R) neu aufgelegt.

Weitere Schwerpunkte der Akademiearbeit bilden traditionell die Kurse zum **betrieblichen Datenschutz**. Im „Grundkurs Bundesdatenschutzgesetz“ (BDSG-I) werden betrieblichen Datenschutzbeauftragten die Grundzüge des für die Wirtschaft geltenden Datenschutzrechts vermittelt. Anhand der „sieben goldenen Regeln des Datenschutzrechts“ (Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit, Transparenz, Datensicherheit und Kontrolle) erhalten die Teilnehmer erste Wegweiser durch die Fülle gesetzlicher Regelungen. „Betriebliches Datenschutzmanagement nach dem Bundesdatenschutzgesetz“ (BDSG-II) und „Technischer Datenschutz/Systemdatenschutz nach dem BDSG“ (SIB) vertiefen diese Grundlage. Großen Zuspruch erfuhr erstmals der neu

eingerichtete dreitägige Lehrgang „Betrieblicher Datenschutz – Kompakt“ (BDK), der die Inhalte der drei vorgenannten Kurse in handlungsoptimierter und praxisbezogener Form zusammenfasst und so den Absolventen einen guten Start in ihre Tätigkeit als betriebliche Datenschutzbeauftragte gibt.

Zunehmende Sensibilisierung im **medizinischen Bereich** in Bezug auf ständige Neuerungen im Gesundheitswesen führten auch bei den Kursen „Datenschutz im Krankenhaus“ (DK) und „Datenschutz in der Arztpraxis“ (AR) zu reger Nachfrage. Der neue Kurs „Gesundheitsdaten in Betrieb und Verwaltung“ (GDB) richtet sich an Personalverantwortliche in Betrieben und öffentlicher Verwaltung sowie an die betriebsärztlichen Dienste der Gesundheitsämter. Pflegedienste und Behinderteneinrichtungen buchen regelmäßig für ihre Mitarbeitenden Fortbildungsveranstaltungen zu Themen des Sozialdatenschutzes (vgl. Jahresprogramm 2011, S. 9).

Das Jahresprogramm der DATENSCHUTZAKADEMIE finden Sie unter



https://www.datenschutzzentrum.de/sommerakademie/

auf der Homepage des Unabhängigen Landeszentrums für Datenschutz (ULD).

Index

P

R

S

T

U

V

W

Z